

pkfcr

Private Key ForCe Repair

概要

本ソフトは、Windows が立ち上がらなくなったとき、その起動ハードディスクから、インターネットバンキング等で使われる電子証明書を吸い上げて別の現に稼動する Windows 上に復旧するものです。もちろん現に稼動している Windows の、あるいは起動する Windows の、起動ハードディスクからでもかまいません。

通常、Windows 内に格納されている電子証明書の鍵コンテナの秘密鍵は Windows DPAPI システムによって暗号化されておりその、その Windows が稼動している時のみそれが解読可能です。よってその Windows が立ち上がらなくなった場合、秘密鍵が解読できないため証明書を復旧することができません。

そこで「pkfcr」は対象ハードディスクから必要な情報(電子証明書と鍵コンテナ等)を抽出し、その鍵コンテナ内の Windows DPAPI システムで暗号化されている秘密鍵とエクスポート可能フラグを独自に解読し、別の稼動する Windows システム上用にこれらを再構築(稼動 Windows 上の DPAPI で再暗号化)してそこに復旧します。

この証明書の復旧には、対象ハードディスクの Windows が起動しないことはさておき、最低限

- ①対象ハードディスク自体がハード的に壊れていないこと
 - ②対象ハードディスクが別の稼動する Windows に接続して読める状態になること
 - ③対象ハードディスク内の電子証明書と鍵コンテナに関連するファイルが壊れていないこと
 - ④復旧対象のユーザーの Windows のログインパスワードがわかっていること
- が必要条件となります。

起動しなくなった Windows と現に稼動している Windows の Version(XP/Win7/Win8 とか x86/x64 とか)が合致する必要はありません。また起動しなくなった Windows より現に稼動する Windows の方の Version が下でもかまいません。但し XP がサポートしない暗号プロバイダを使う証明書や鍵コンテナを XP で扱おうとするとエラーになります。

ドライブ自体が暗号化されている場合(BitLocker 等)は暗号解除して読める状態にしてください。本ソフト自体は BitLocker 等の暗号解除には対応していません。

ファイルに暗号化がしてある場合で、それが Windows の「暗号化ファイルシステム(EFS)」の場合は、それを解読する EFS 証明書(と鍵コンテナ)を本ソフトで復旧することで対応できます。すなわち EFS 証明書を現に稼動するシステム上に再構築すれば、立ち上がらなくなった Windows 上の暗号化ファイルは読めるようになります。尚、EFS 証明書は通常そのユーザー名で作成されていますのでそれを目安にそれを見つけることになります。

復旧対象ユーザーアカウント環境は、
①ローカルユーザーアカウント
②ドメインユーザーアカウント
③マイクロソフトユーザーアカウント(Windows8 以降導入の)
に対応します。

また、ユーザーエリアではなくローカルマシンエリアに保存された証明書と鍵コンテナにも対応します。ローカルマシンエリアの証明書、鍵コンテナを復旧するには、ユーザーログインパスワードは無関係のためそれを知っている必要はありません。

復旧対象は起動しなくなったハードディスクに限らず、要は証明書を復旧するに必要な情報を格納しているものがありさえすればよいので、例えば現に稼動している Windows 上の起動ドライブ(C:等)も対象になり得ます。また復旧対象はドライブである必要はなくディレクトリでもかまいません。

本ソフトには、復旧対象から証明書を復旧するに必要な情報を一括して引抜きバックアップする機能があります。その引抜いたデータを復旧対象に証明書を復旧する場合は、引抜いたデータの入ったディレクトリが復旧対象にされることになります。

また「pkfcr」は鍵コンテナ内の秘密鍵エクスポート可能フラグを解読できますので、起動しなくなった Windows や現に稼動する Windows 上の電子証明書の秘密鍵エクスポート不可の状態を可能化することができます。これは姉妹ソフトでこの秘密鍵エクスポート不可を可能化するソフトの「pkfcx」とは全く違う原理でこれを実行します。

動作確認環境

Windows 環境でのみ動作します。以下の OS 環境であればそれ以上の動作要件はありません。

対応プラットフォーム x86 (IA-32) と x64 (その他のプラットフォームには対応していません)

x86 環境

WindowsXP-SP3 Windows2003-R2-SP2 Windows2008-R1-SP2

Windows7 Windows7-SP1 Windows8 Windows8.1

x64 環境

Windows2008-R2-SP1 Windows7 Windows7-SP1 Windows8 Windows2012 Windows8.1

これ以外の OS 環境では動作検証されていません。x64 環境で x86 版は (WOW64 でも) 動作しません。

同梱ファイル

pkfcr本体 pkfcr32.exe (x86用実行ファイル) pkfcr64.exe (x64用実行ファイル)

その他説明書(本ファイル。尚、本ファイルを上記実行ファイルと同じディレクトリに置いてください。)

インストール

インストール作業は不要です。実行ファイルを直接起動してください。

尚、バージョンアップ時には本ソフトを起動後一旦「完全終了」ボタンで終了してから再起動してください。

アンインストール

本ソフトは起動するとシステムのいくつかのレジストリを使用する他、テンポラリフォルダでいくつかのファイルを生成します。しかし「完全終了」ボタンを押して終了することでこれらを削除し導入前の環境に戻せます。すなわちアンインストール作業は不要です。

「完全終了」ボタンによる終了は、原則本ソフトによるシステムへの残存物を全て削除しますが、本ソフトが試用制限を設けている関係上、試用関係情報のみ例外としてシステムに残存させてもらっています。尚、本ソフトの使用レジストリは以下で画面位置等を記録しています。

HKEY_LOCAL_MACHINE\SOFTWARE\pkfcr KEY_LOCAL_MACHINE\SOFTWARE\pkfcr_regist

シェアウェア・試用・試用中の制限について

本ソフトは起動回数「10 回まで」、インストール後「7 日間」試用することができる「シェアウェア」です。

その間で、お使いの環境での動作確認を行っていただき、継続使用の場合はご購入ください。

「電子証明書復旧機能」以外は無償で継続使用できます。

尚、試用中では、復旧した証明書の秘密鍵エクスポートが不可となります。

金額・支払方法について

ソフト本体価格(消費税別)5,600 円です。支払方法は原則「ベクタシェアレジ」のみとなります。

ベクタシェアレジがなんらかの事情で利用できない方は下記メールアドレスへ連絡ください。

個別に折返し、銀行振込による方法をご連絡します。

連絡先

作者への連絡先は下記のとおりです。

ハンドル 丸太

メールアドレス gqcr2rd9k@arion.ocn.ne.jp

その他注意事項

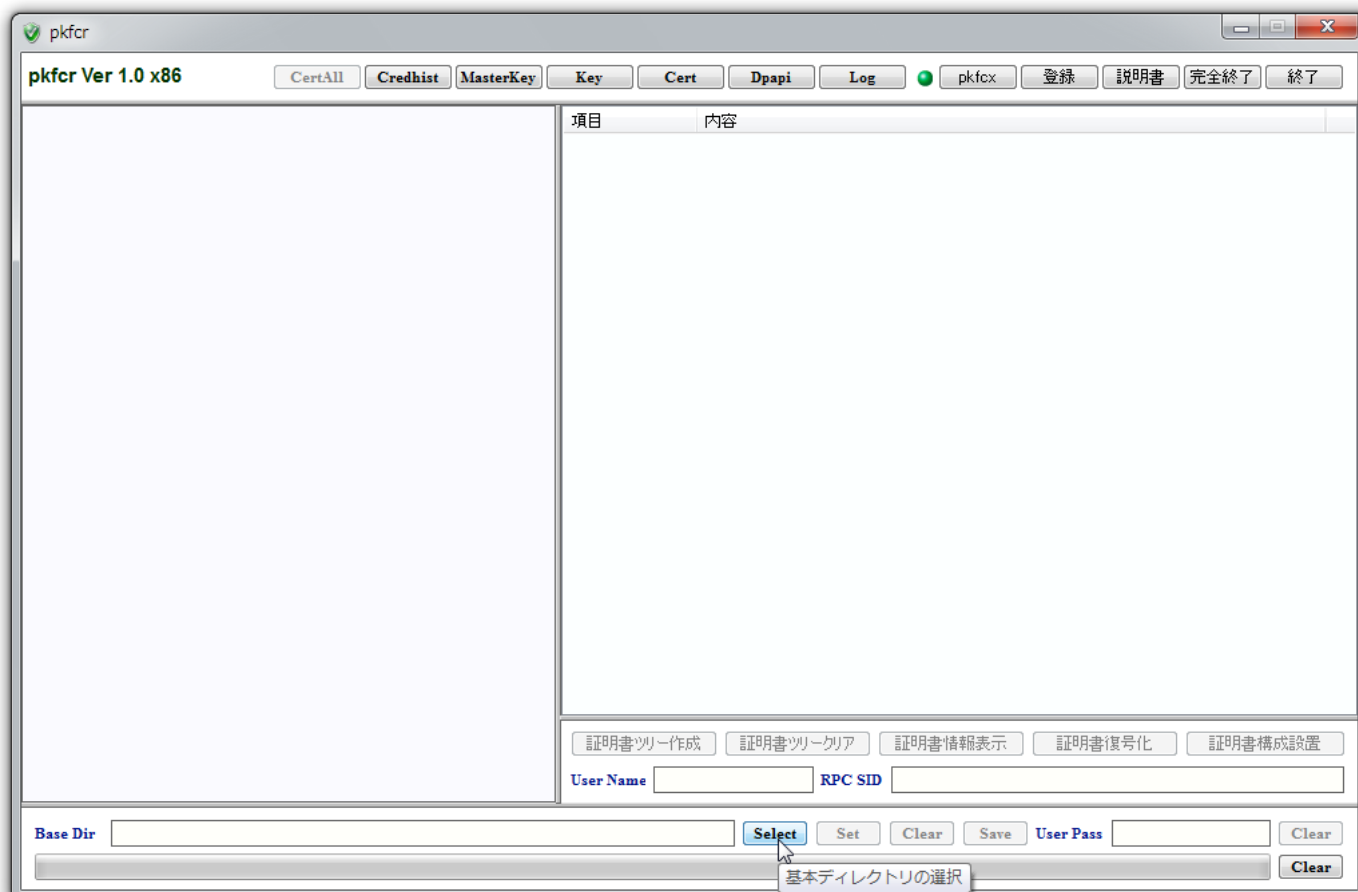
- ① ドライブを暗号化するソフトで「システムドライブ」全体を暗号化してある場合「pkfcr」は試用回数及び期間の計測を誤り、初回起動時いきなり試用回数または期限超過になります。そのような環境では「試用」できないことをご了承ください。
- ② システムに、物理ハードディスクが最低 1 台接続されている必要があります。具体的には Windows システム上に「¥¥.¥PhysicalDrive0」のシンボリックリンクが存在している必要があります。

簡単「電子証明書」復旧方法

ここでは仮に Windows7-SP1 x86 環境の例で説明します（他の環境では多少の違いがありますが同様です）。

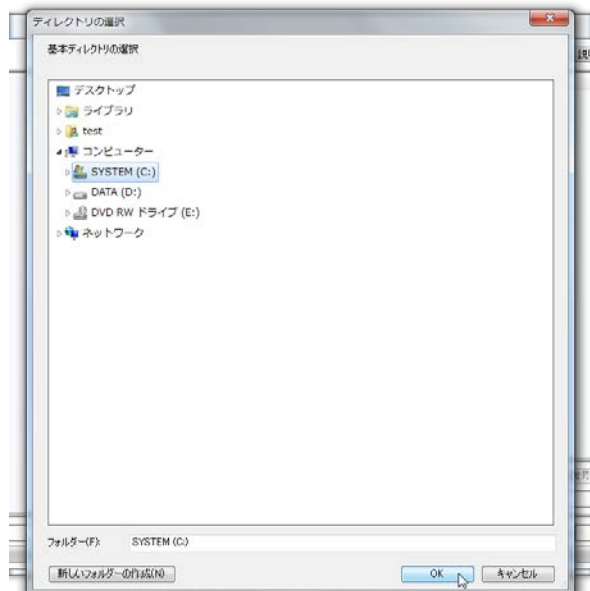
復旧対象の選択

前もって復旧対象のハードディスクをシステムから読める状態にしてください。すなわち起動しなくなった Windows 等の起動 HD を現に稼動する Windows に(USB 変換あるいはダイレクト接続等で)接続してください。
そして本ソフトを起動します。

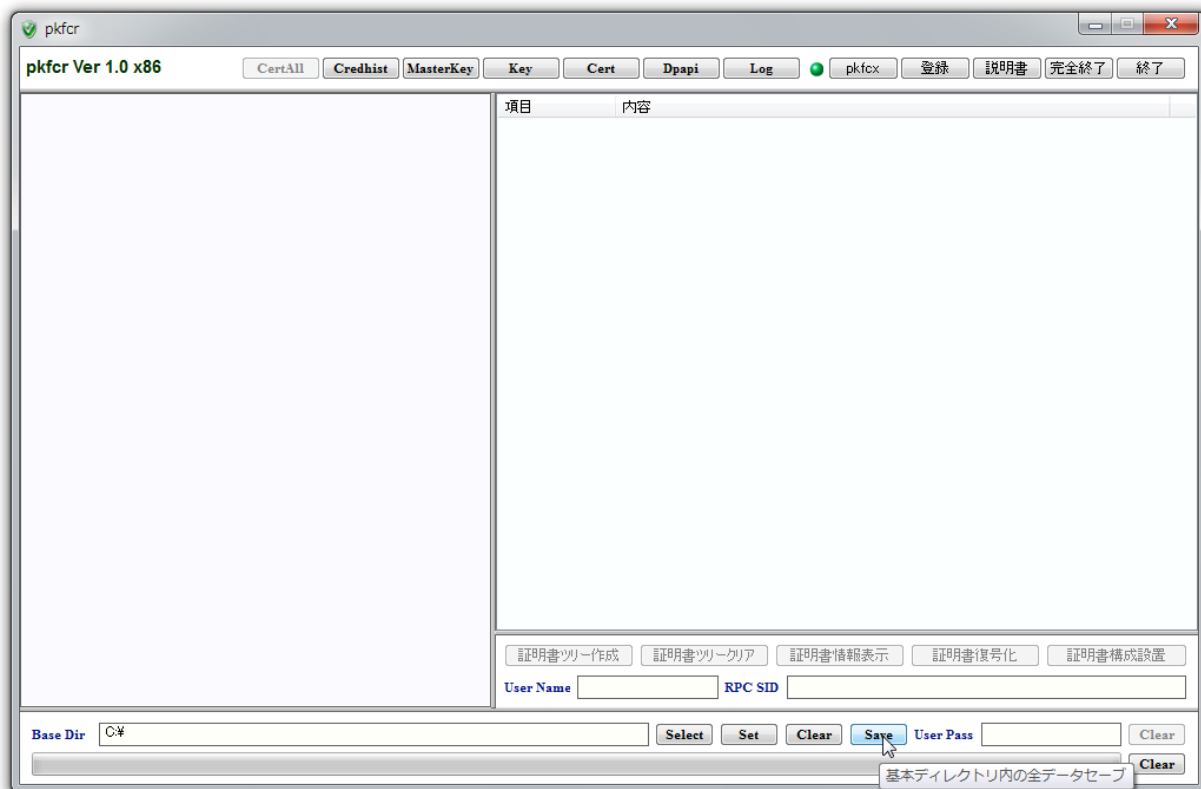


下方の「SELECT」ボタンを押下し、復旧対象のドライブ(ないしディレクトリ)を選択してください。通常 D: ドライブ以降のドライブ名になるかと思われますが、以降の説明では便宜上「C:」が復旧対象ドライブと仮定して話を進めます。(実際 C: を選択すると現稼動システムの証明書を復旧することになりますので、その行為に実用性はありません。)

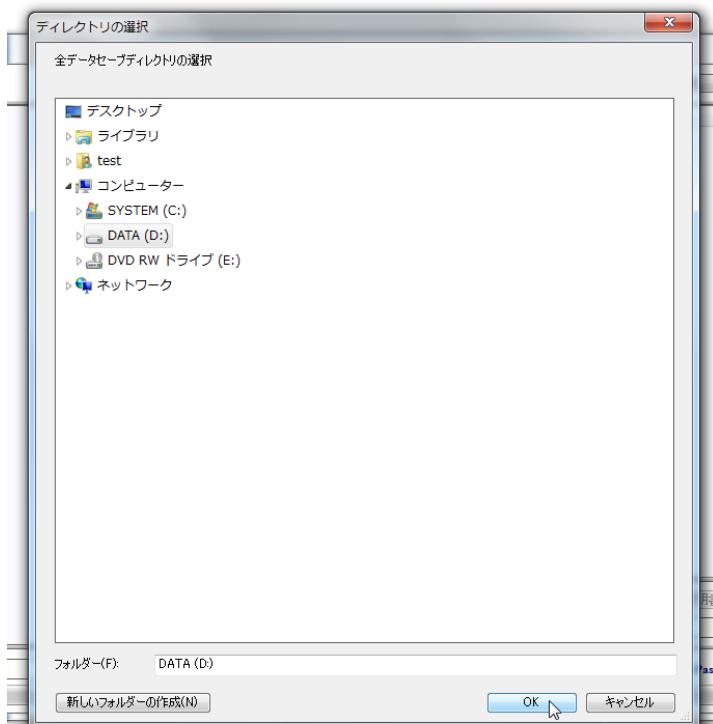
下図のように「基本ディレクトリの選択」になりますので、そこで復旧対象を選択し「OK」ボタンを押します。



続いて「Save」 ボタンを押します。



下図のように「全データセーブディレクトリの選択」になりますので、適宜な場所を選択します。下の例では「D:」ルートディレクトリを選択しています。ここで「OK」 ボタンを押すと直ちに「全データセーブ」が実行されます。

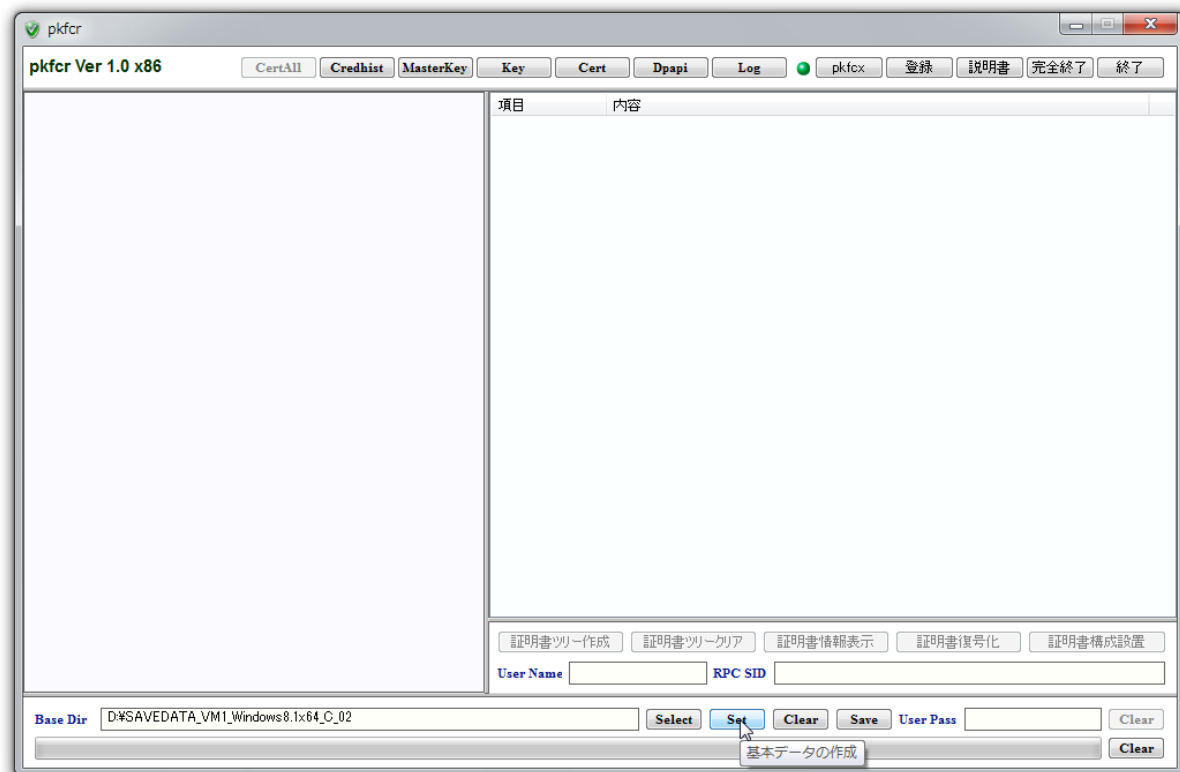


ここで「全データセーブ」とは、先に指定した「基本ディレクトリ」内の復旧に必要な全ての対象(ファイル類)を別の場所に保存する、という作業になります。この例では「C:ドライブ」内の復旧するに必要な全てを「D:ドライブのルートディレクトリ」に保存することになります。

ここであえて「全データセーブ」しなくても「基本ディレクトリ」に指定したターゲット(ここでは「C:ドライブ」)に対し直接の復旧作業は行えます。その場合は「基本ディレクトリ」を選択した後「Save」せずに左の「Set」ボタンを押して次ページ中段の説明に飛んでください。

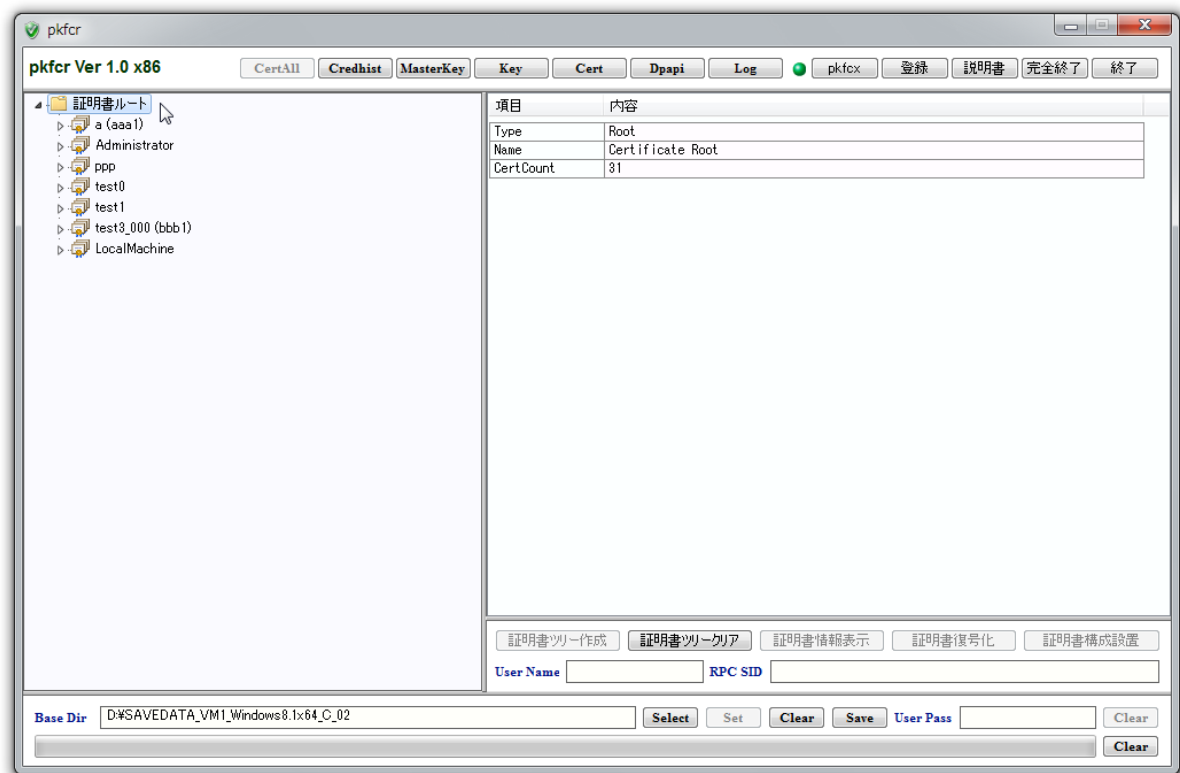
ただ、手元 HD 内(ここでは「D:ドライブのルートディレクトリ」)に「全データセーブ」しておけば、以降そのセーブデータを対象とすればよくなり、復旧対象の HD を繋ぐ必要がなくなります。すなわち「全データセーブ」後は復旧対象の HD はもう切り離してかまいません。

「全セーブデータ」は指定したディレクトリの下に独特の名前のディレクトリでまとめられ保存されます。この名前は本ソフトが決めてしまうのでユーザーは選択できません。(ユーザーがこれをリネームすることはかまいません。) 続いて先に設定した「基本ディレクトリ」(この例では「C:」)を、いま「全データセーブ」したディレクトリに切り替えます。たとえば「SAVEDATA_VM1_Windows8.1x64_C_02」の様な名前で先ほど保存した「D:ドライブのルートディレクトリ」にセーブデータが入っているので、再度「Select」ボタンを押し、この例では「D:\\$AVEDATA_VM1_Windows8.1x64_C_02」ディレクトリを選択してください。

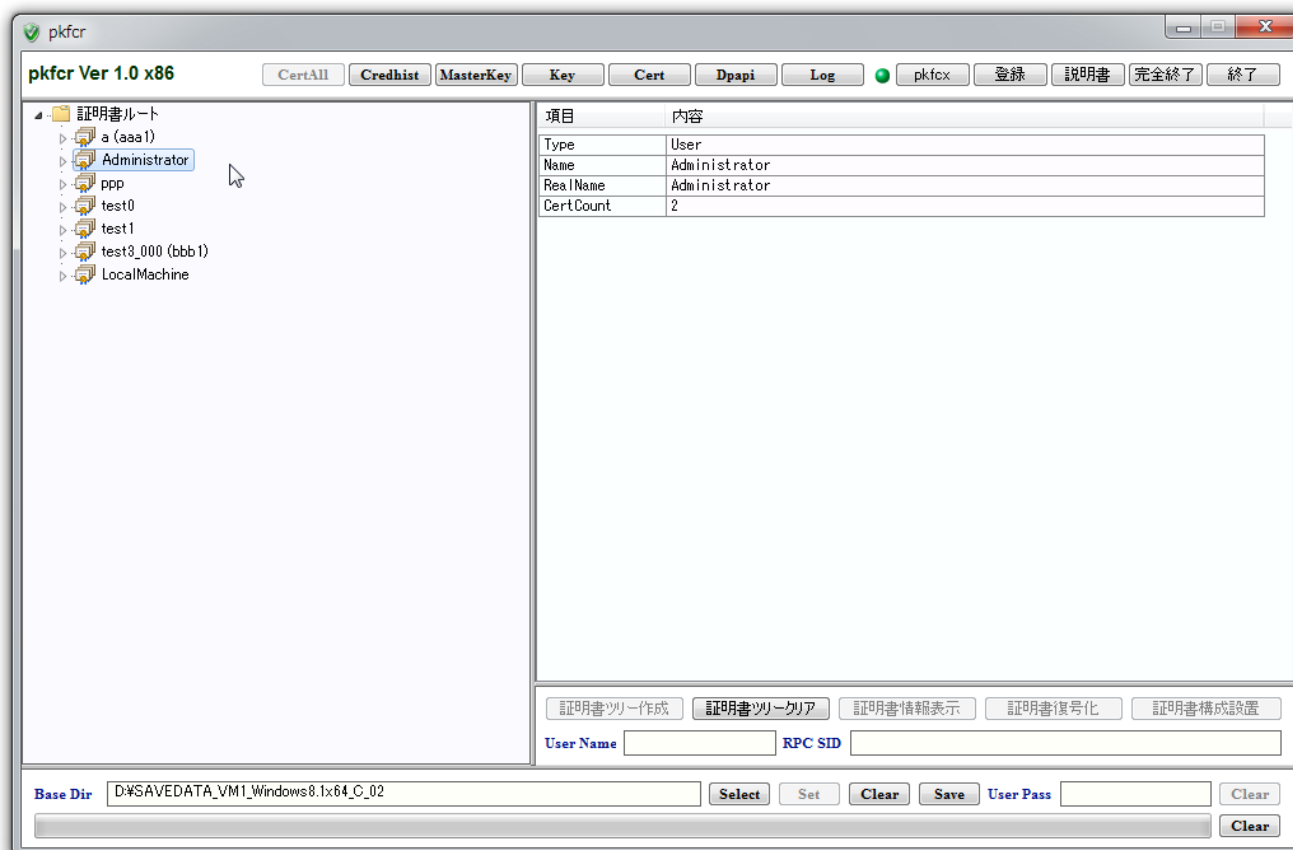


上図のようになりますので、「Set」ボタンを押してください。
尚、右の「Clear」ボタンは「Set」の解除になります。さらに押すと「Select」の解除になります。

下図のように、復旧対象データを解析して必要な情報を表示します。もし「Select」したドライブ・ディレクトリが復旧対象として不適格だった場合、ここで何も表示されません。ただ通常は、システムドライブ(だったもの)を指定しさえすれば不適格になることはありません。

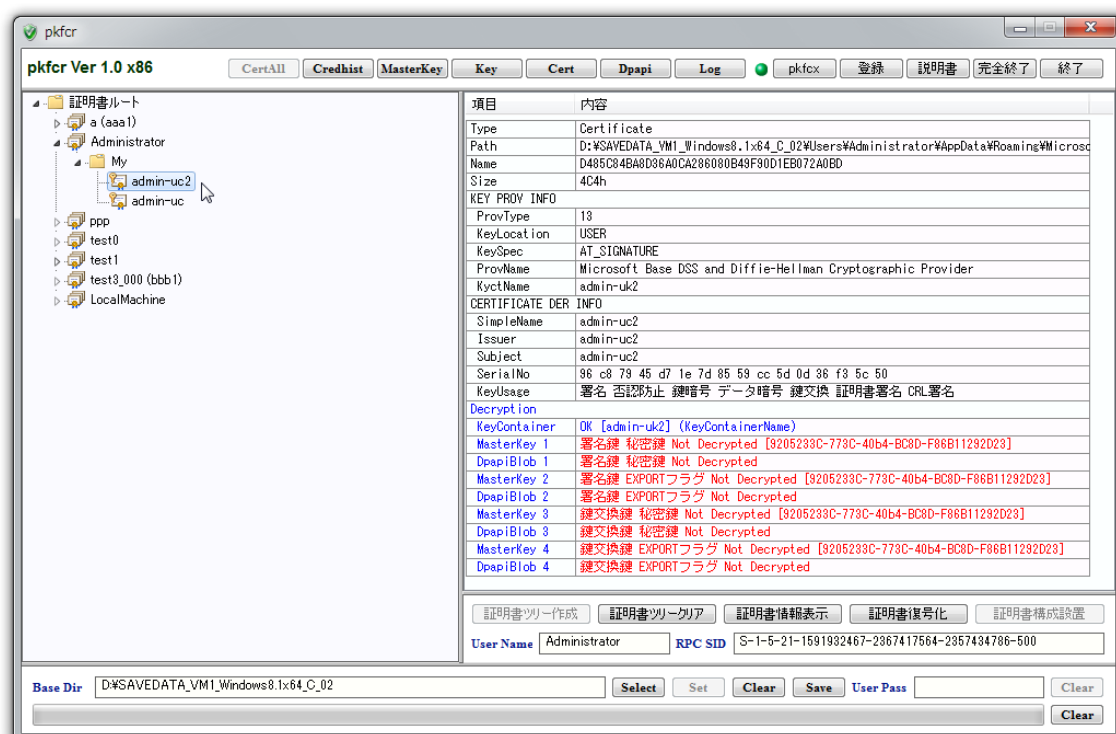


ここで画面左方にツリー表示されているのは復旧対象 HD 内の対象ディレクトリから見つかった全ユーザーです。

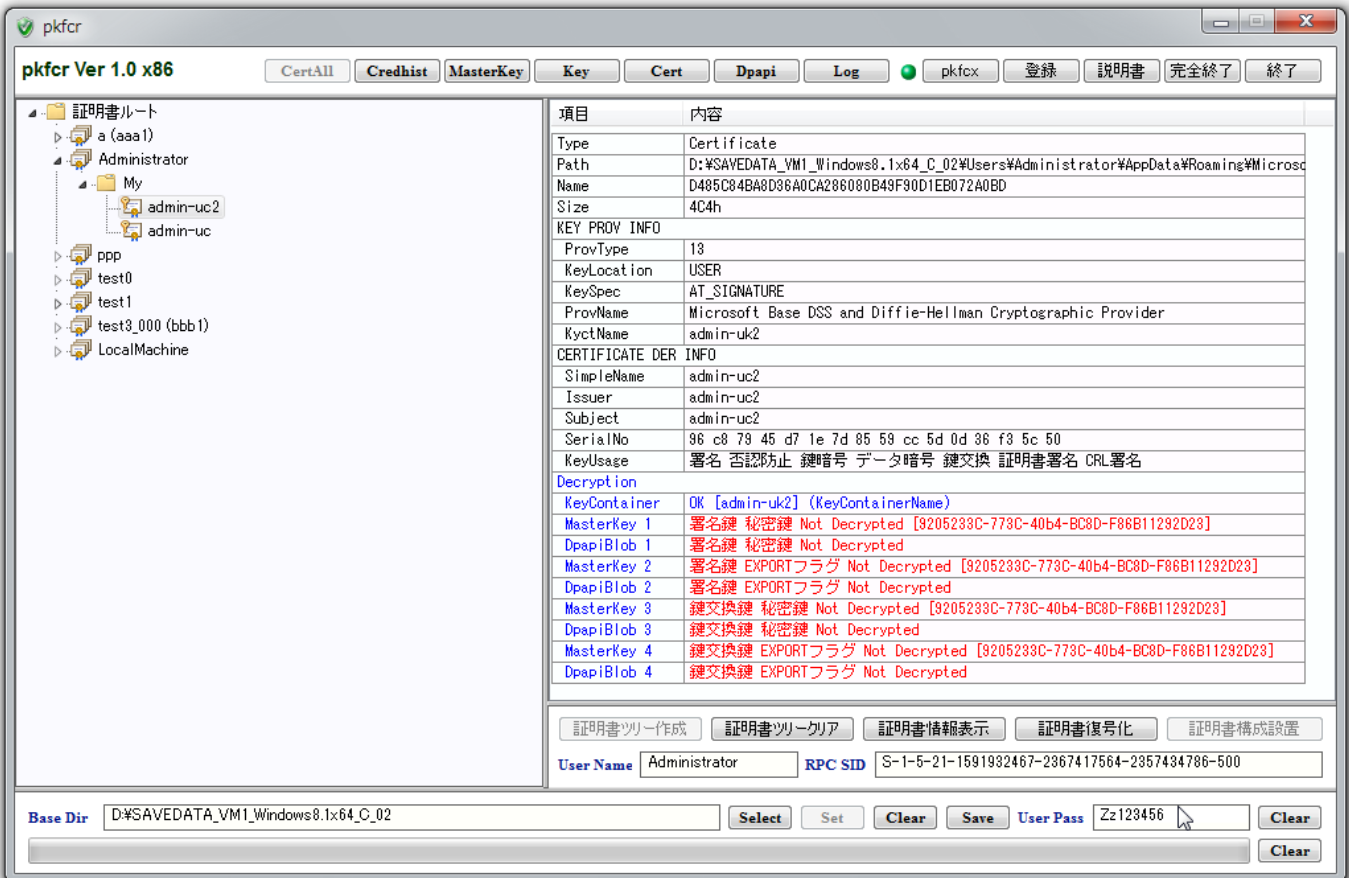


ここで表示されるユーザー名は、一般的に「C:\Users(エクスプローラでは「C:\ユーザー」と表示されます)」ないし「C:\Documents and Settings」ディレクトリ直下にある各ディレクトリ名(各ユーザーに割当てられるディレクトリで以降「ユーザーディレクトリ」と呼びます)を参考に表示しています。しかしユーザー名を変更している場合、このディレクトリ名とユーザー名に齟齬が生じます。上図の例で「a(aaa1)」と表示されているのは、当初は「a」という名前(ユーザーディレクトリ名も「a」)だったが、その後ユーザー名が変更され現在のユーザー名は「aaa1」であることを示しています。尚、表示されるユーザーは当然に環境によって異なりますが以下この例で説明をしていきます。

続いて、上図のようにユーザー「Administrator」を選択し左横の白い三角マークをクリックすることで、下図のようにそのノードを展開していただきます。そのユーザーに証明書があれば下図のようにそれが表示されます。指定したユーザーがそのユーザーエリアの「個人」という場所に証明書を「2 個」登録してあった場合にこのような画面となります。

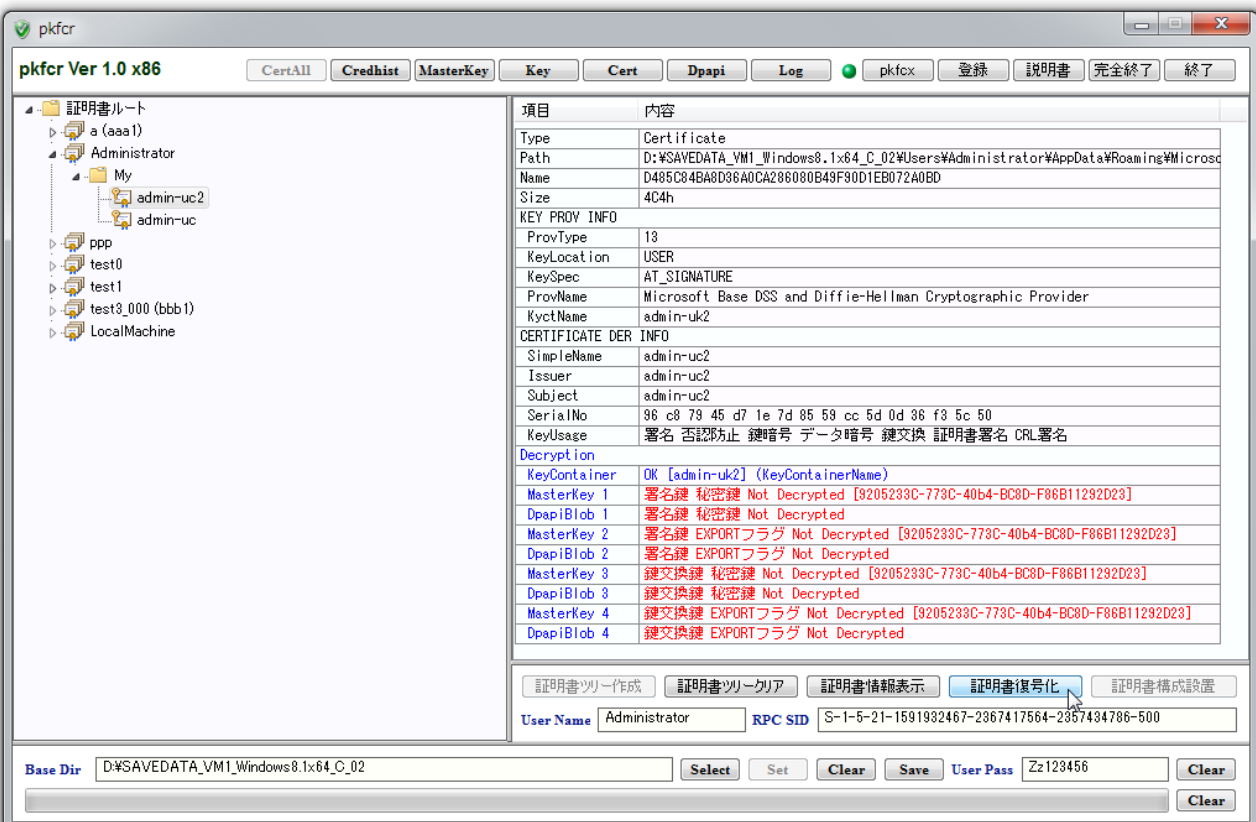


ここでは「admin-uc2」という証明書が存在し、いまそれを選択表示している状態です。

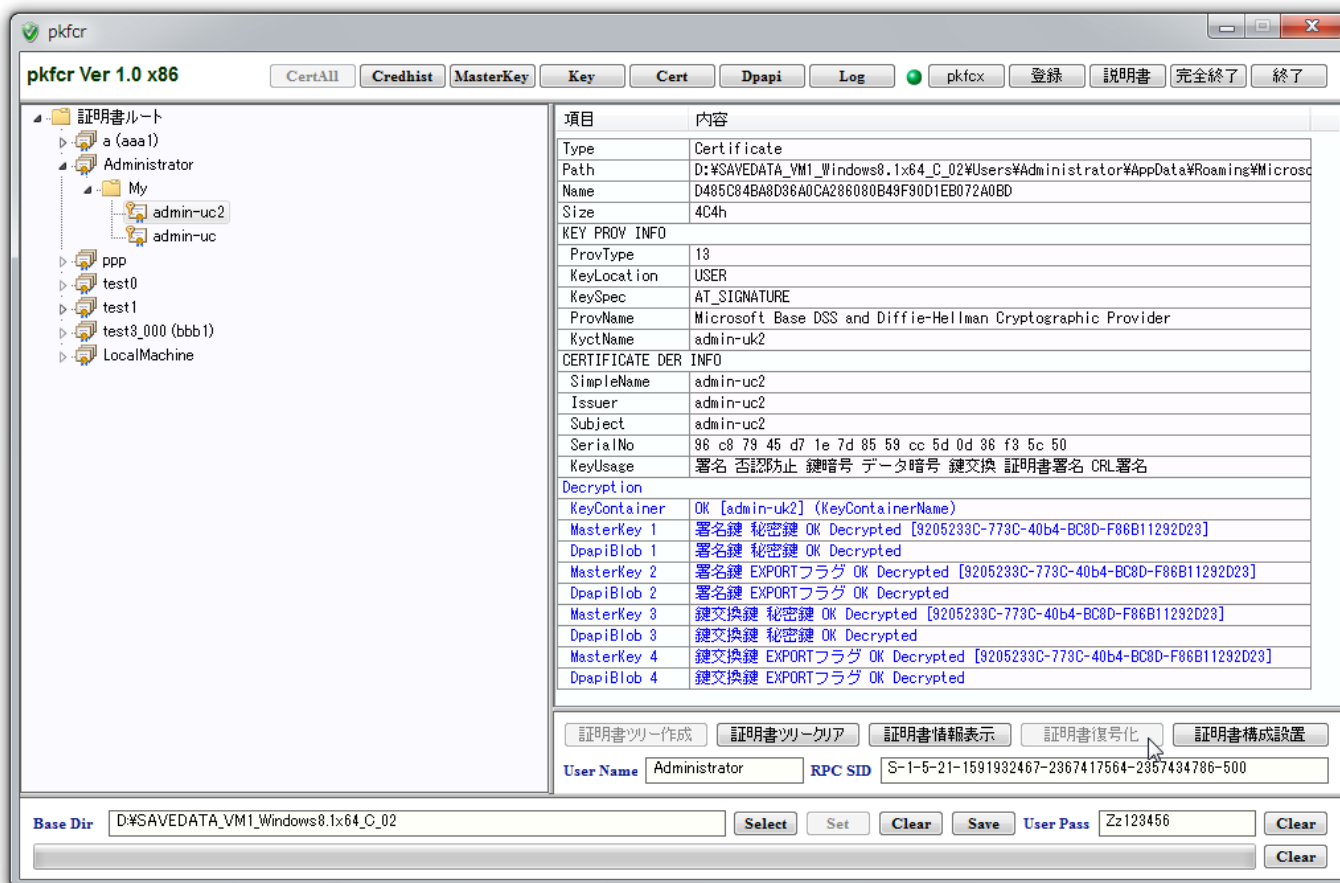


ここで、「Administrator」ユーザーの Windows ログインパスワードを上図のように下部右方に入力してください。ここでは仮に「Zz123456」として話を進めます。もしログインパスワードを設定していない(パスなし)ユーザーだったなら入力欄は空欄にします。右の「Clear」ボタンはパスワードをクリア(空欄に)します。

尚、パスなしユーザーではなく、ログインパスワードがわからない場合は「pkfcr」ではどうにもなりません。ここで話は終わりになります。(ただログインパスを割出すツールが世には存在しますのでそれで見つけ出すということは考えられます。)下図のように「証明書復号化」ボタンを押してください。

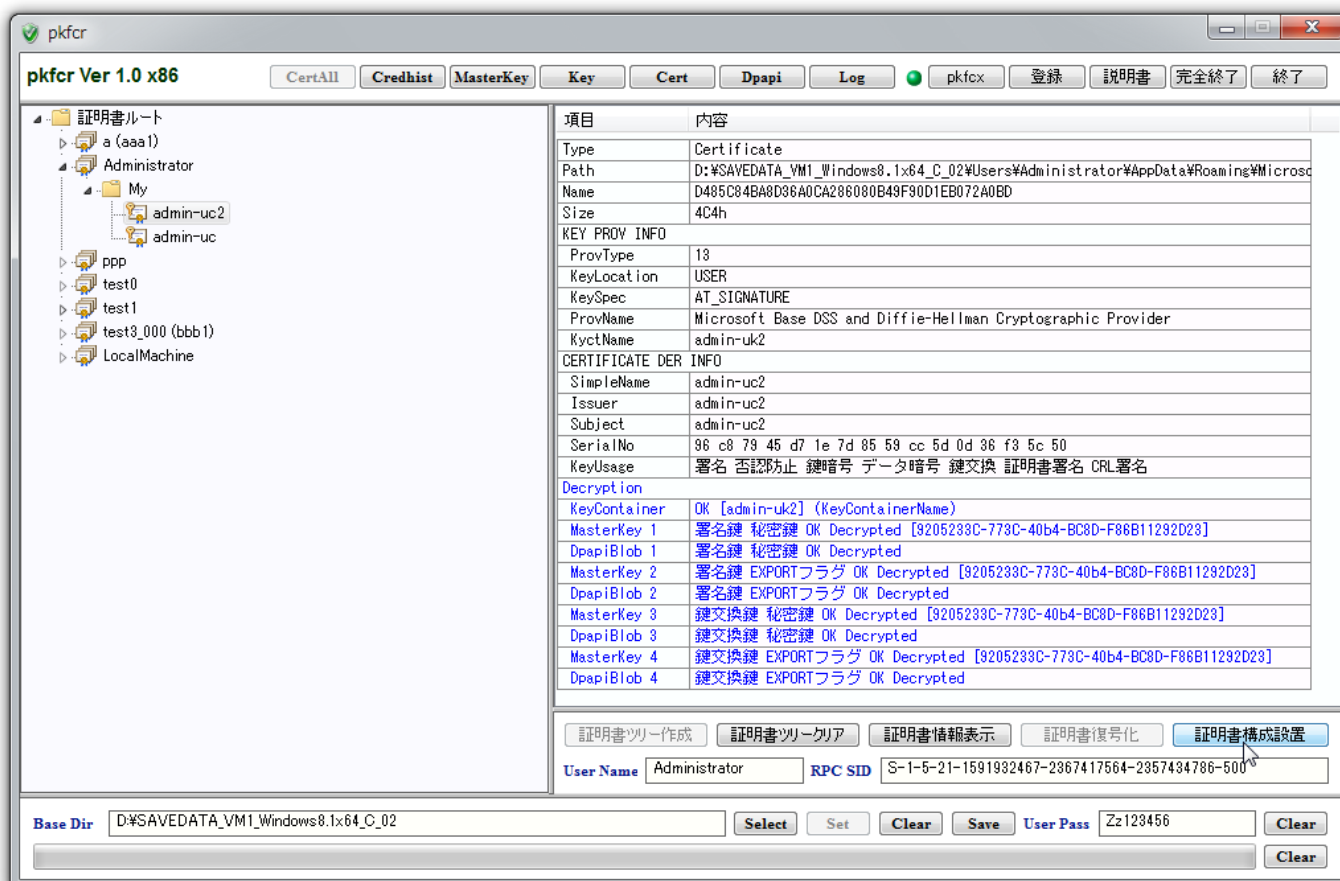


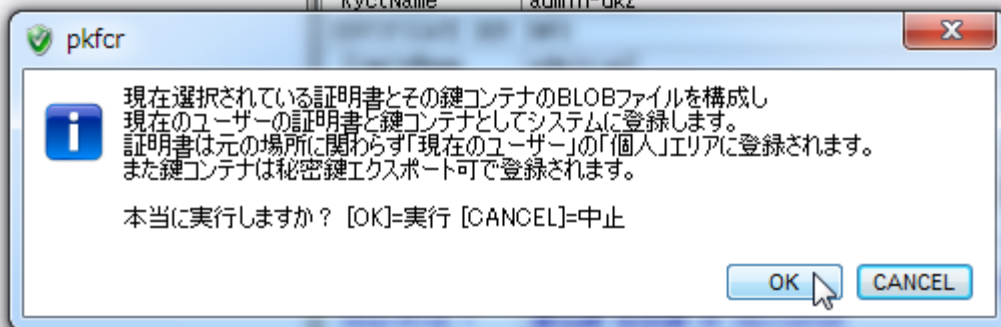
パスワードが正しければ以下のように「復号化」が成功します。パスワードが違っている場合、ここでエラーとなり先に進めません。



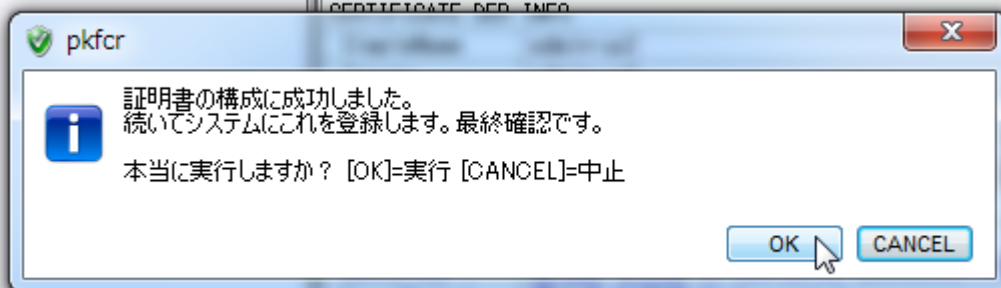
上図のように「赤色」表示だった部分が「青色」になっていることを確認してから、

下図のように「証明書構成設置」ボタンを押してください。

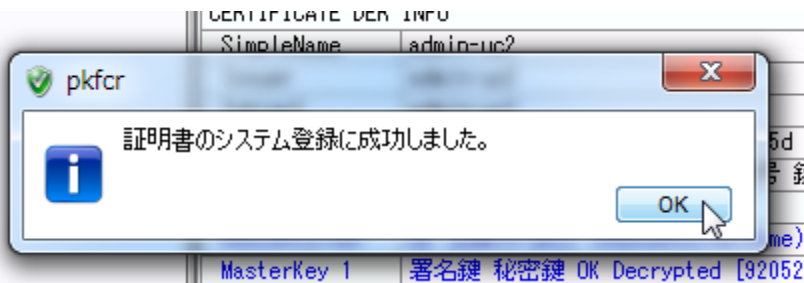




上図のような表示が出ますので「OK」ボタンで先に進んでください。

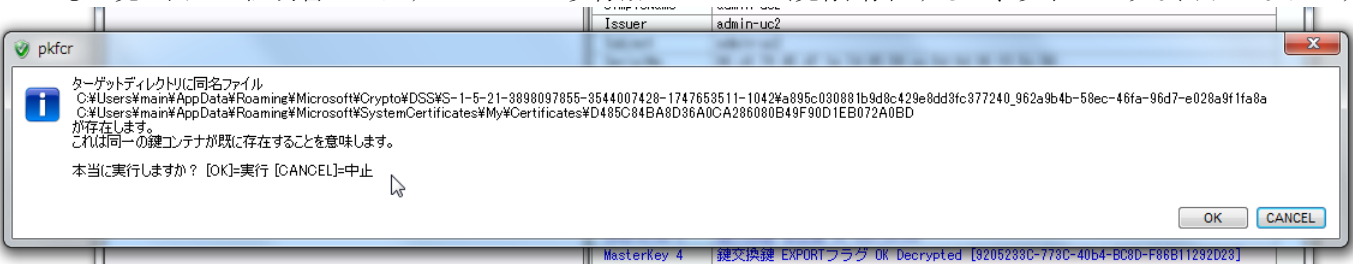


続いて上図のような画面になります。この時点で証明書が復旧できる体制が整っています。ここで「OK」ボタンを押せば現在稼働中のシステムにそれが登録されますし、ここで「CANCEL」すれば全てが中止されます。



「OK」で進んだ場合、このような表示が出て証明書の復旧に成功します。

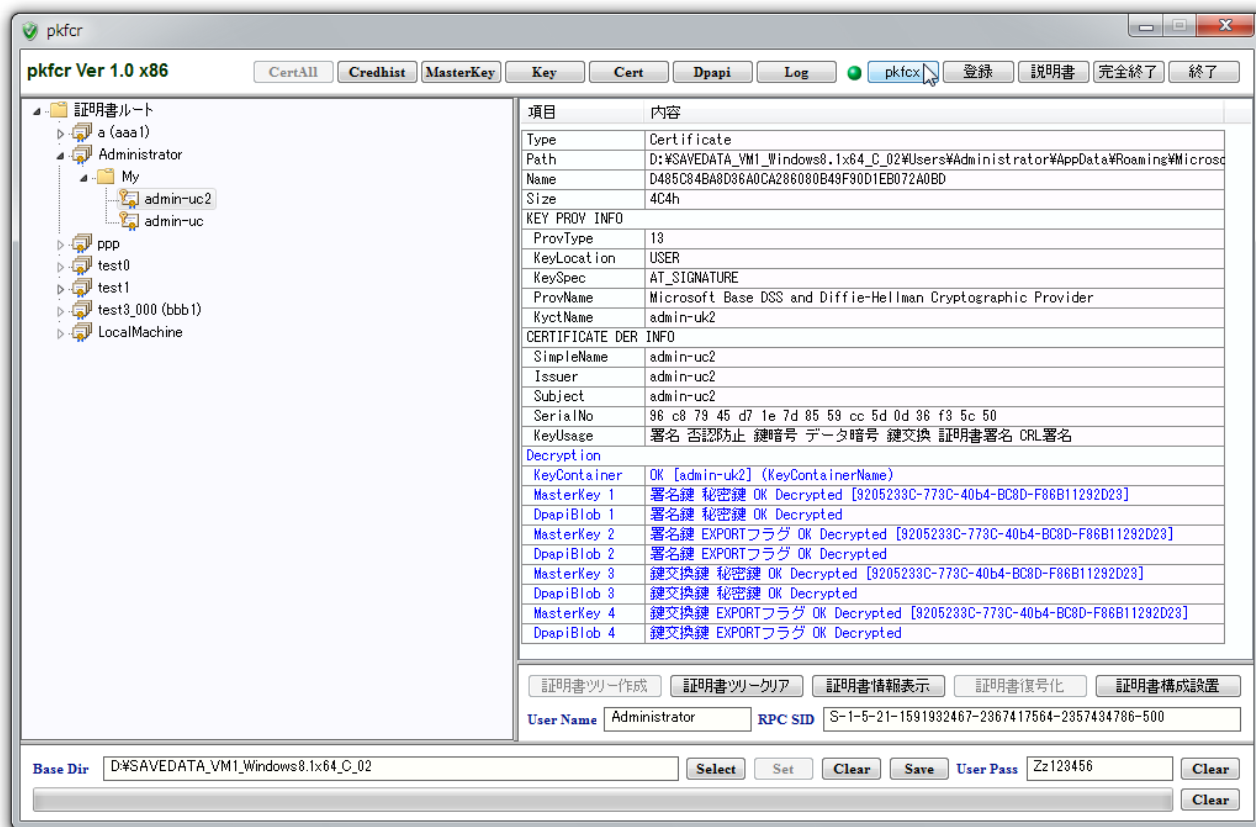
ここでもし既に同一の証明書または鍵コンテナが現稼働システムに(既存)存在すると、以下のような表示となります。



現システムに存在するこれらに上書きしてもかまわないなら「OK」で進み、中止するなら「CANCEL」します。このような事態は、二重に証明書を復旧しようとしたような場合にしか起こりませんので、通常はここで「CANCEL」で進みます。もし二重復旧の心当たりがないのにこのようになった場合、別のシステム上で復旧するのが無難です。ここで既存存在とは、正確には同一の証明書、鍵コンテナ存在というより、同一ファイル名の存在を示し、通常起こり得ないことですが、別の証明書ないし鍵コンテナなのに、たまたまファイル名が重複してしまうということは有り得ます。

「基本ディレクトリ」の選択で「C:ドライブ」を選択して処理を進めた場合、現に稼働しているシステム上の証明書と鍵コンテナの復旧をしようとするに他なりませんので、必ずこの局面で、既存存在となります。しかし、この処理はオリジナルの秘密鍵エクスポート不可属性を解除して行うので(但しこれは本ソフト購入登録時のみの動作となります)、もし現稼働システム上の証明書の秘密鍵エクスポート不可を解除したい場合、ここで上書き続行することで事実上「エクスポート不可」を解除できることになります。

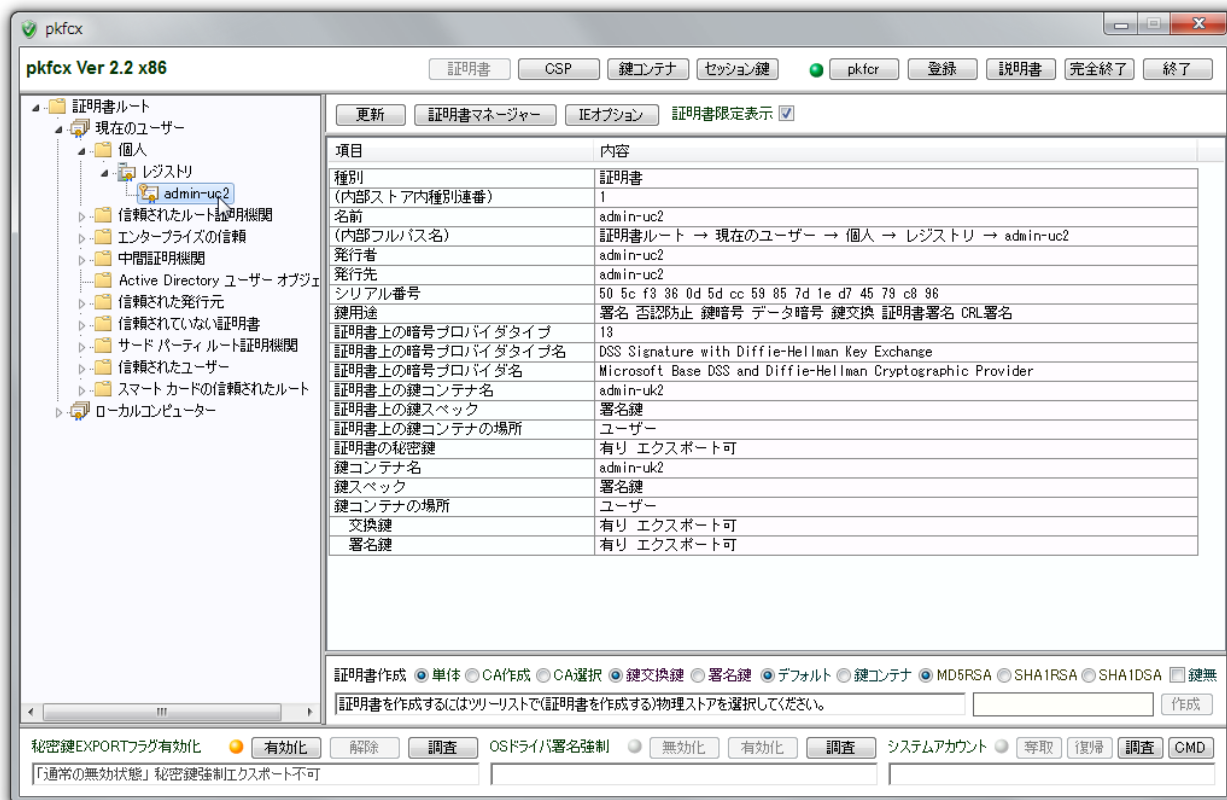
ここで OS 付属の「certmgr.msc(証明書管理ソフト)」か、姉妹ソフトの「pkfcx」を起動します。



ここでこれらを起動する理由は、証明書が確かに現稼働システム上に復旧されたかを確認するためだけですので、実際は不要です。尚、上図「pkfcx」ボタンは「pkfcx Ver2.2」を一度以上起動した環境でのみ有効です。

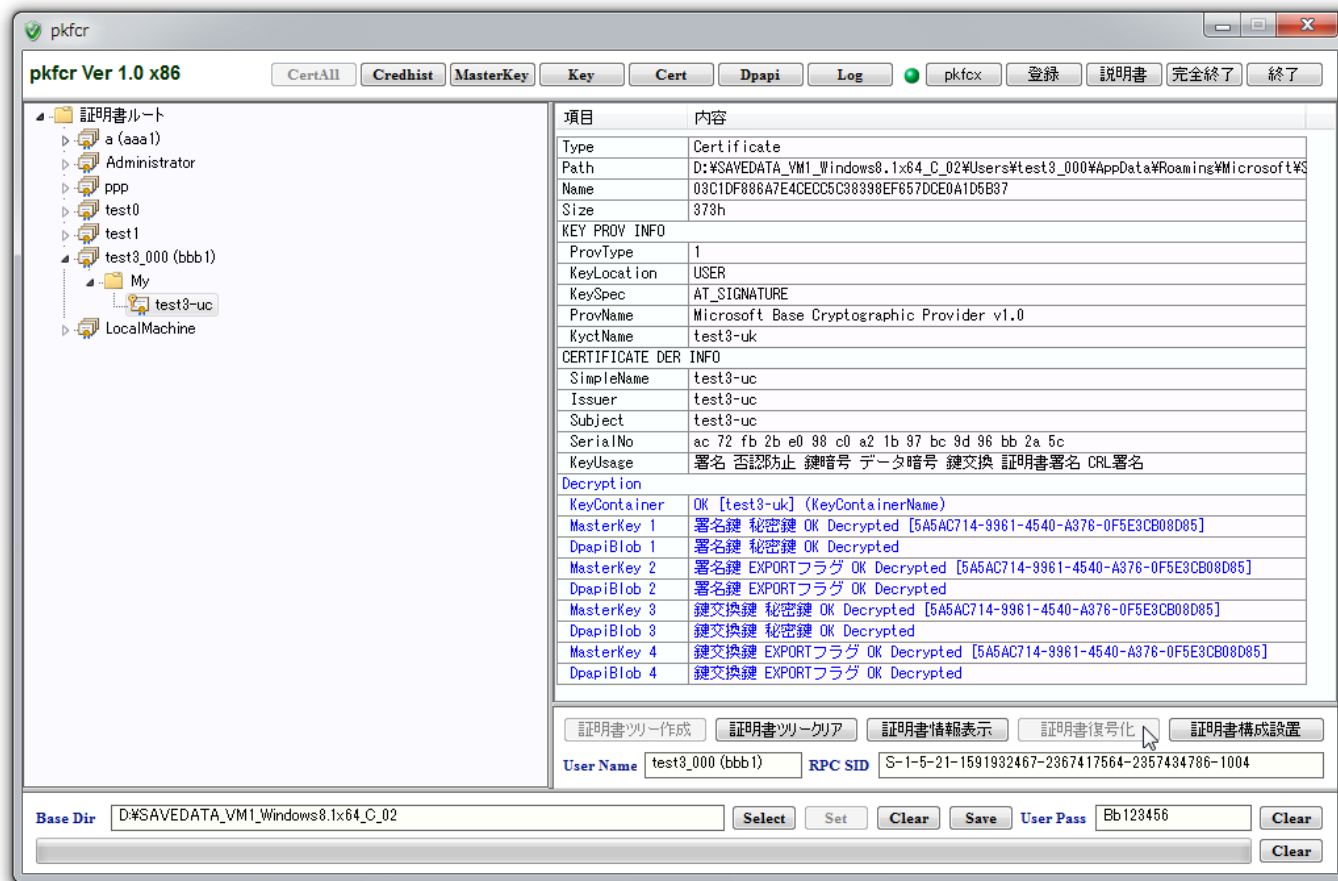
下図のように「pkfcx」上でも、確かに先の証明書「admin-uc2」が復旧されたことが確認できました。後はこのまま使うなり、秘密鍵付でエクスポートして別マシンに移動するなりします。

ここで元の証明書が「秘密鍵エクスポート不可」だったとしても復旧後は自動で「エクスポート可」になることに注意してください(但しこれは本ソフト購入登録時のみの動作となります)。エクスポートできなくて意味がないのでこのような仕様になっていますが、これをこのまま放置することはセキュリティ上危険ですので、適宜エクスポート不可に(pkfcx 等で)してください。



他のユーザーの証明書についても同様に処理できます。下図のように各ユーザーごとに下部左方の「UserPass」を適宜に設定しなければ「証明書復号化」が失敗するので注意が必要です。

ユーザーの「LocalMachine」は正確には「ユーザー」ではなく、ローカルマシンエリアに保存された証明書を示すものです。この場合その証明書の復旧にはパスワードは不要です。パスワード欄が空欄でも何か入力されていても関係なく「証明書復号化」は成功します。



画面最下部にはプログレスバーがあります。「pkfcr」では一定のアクション(全データセーブ等)で時間が掛かる場合これを別スレッドで実行します。そのとき進行状況をプログレスバーで表示します。プログレスバー右の「Clear」ボタンはプログレスバーをクリアしますが、プログレスバーの進行状況は100%に達した後数秒後に自動でクリアされますのでほとんどこのクリアボタンを使うことはありません。

電子証明書の復旧原理の詳細

ここでは「pkfcr」の操作方法詳細を理解するために最低限必要となり、証明書を復旧するための技術の根幹をなす Windows の DPAPI システムの深部を説明します。

DPAPI 総論

壊れた Windows 上の証明書を復旧するには、起動ハードディスクから、

1. 対象の証明書ファイルを見つけ、
(但し、ローカルマシンエリアに保存された証明書の場合はファイルではなくレジストリに存在します)
2. それに使われた鍵コンテナファイルを見つけ、
(鍵コンテナは保存された場所がユーザーエリアでもローカルマシンエリアでも、場所は違いますがファイルとして存在します)
3. その中の秘密鍵を Windows の DPAPI で解読する必要があります。

しかし Windows の DPAPI システムはその Windows が現に稼動していないと使えません。
原則としては、別の Windows からでは解読できないのです。

DPAPI とは Windows の標準機能で、ユーザーが簡単にデータを暗号化、復号化することができる API の総称です。
DPAPI はユーザーに開放されているだけでなく、OS 自身が内部の随所でその機能を使っており、特に鍵コンテナ内の秘密鍵とそのエクスポート許可フラグについてこれを DPAPI 暗号化しています。

DPAPI にはユーザーモードとローカルマシンモードが存在します。
ユーザーモードの DPAPI で暗号化されたものは、その Windows が稼動していることはもとより、そのユーザーがログインしている状態でないと復号化できません。
ローカルマシンモードの DPAPI で暗号化されたものは、そのマシンにログインしている全てのユーザーが復号化できます。
いずれにせよ暗号化が行われたその Windows マシンが稼動していることが前提となります。

稼動しない Windows の DPAPI を解読するには DPAPI のエミュレーションが必要であり、
本ソフトはそれを実装しています。

ユーザーモードの DPAPI では「ユーザーがログインしている状態」に 3 種類があります。
「ローカルマシンにローカルユーザーとしてログインしている状態」
「ドメインコントローラーに管理されたマシンにドメインユーザーとしてログインしている状態」
「ローカルマシンにマイクロソフトアカウントでログインしている状態(Windows8 以降)」
これらそれぞれで DPAPI の挙動は違うためそれら全てをエミュレーションする必要があります。
もちろん、ユーザーモード DPAPI とローカルマシンモード DPAPI でも挙動は違います。

DPAPI のエミュレーションを行うといっても、
証明書と鍵コンテナの情報以外にさらに一定の前提情報が必要となり、
その情報はその Windows の起動ドライブ内にファイルとして存在します。
レジストリ情報が必要なこともあります、レジストリも実体はファイルですので結局、
全ては起動ドライブ内のファイルに帰結します。

証明書

Windows の証明書は、概念的にユーザーエリアかローカルマシンエリアに保存されますが、その実体 (CERTBLOB) は以下の場所に存在します。

ユーザーエリアの証明書

C:\Users¥(ユーザー名)¥AppData¥Roaming¥Microsoft¥SystemCertificates¥My¥Certificates 内の各ファイル
但しこの場合、ユーザーエリアの個人 (My) というストアに保存された証明書

ローカルマシンエリアの証明書

レジストリ HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥SystemCertificates¥My¥Certificates 内の各キー
その値「Blob」が実体
但しこの場合、ローカルエリアの個人 (My) というストアに保存された証明書
そしてレジストリ HKEY_LOCAL_MACHINE¥SOFTWARE の実体は
C:\Windows¥System32¥config 内のファイル SOFTWARE

証明書 BLOB (CERTBLOB) は全く暗号化されていません。その中には証明書の情報の全てが入っており、対応する鍵コンテナの名前情報が入っているためこれを頼りに、その対応する鍵コンテナを見つけます。

上記「SystemCertificates¥My¥Certificates」という場合、「個人」というシステム定義のストアに証明書がある、ということになり、通例多くの証明書はここに入りますが、このシステム定義のストアには他にも色々ありますので (My/Root/CA/trust 等)、場合によってその他の証明書ロケーションを探さなければならないこともあります。

証明書には対応する鍵コンテナ (秘密鍵) のない、すなわち公開鍵だけの証明書と、対応する鍵コンテナのある証明書があります。証明書 BLOB 自体は暗号化されておらず、暗号化されているのは鍵コンテナの秘密鍵だけですので、鍵コンテナのない証明書は特段の解読作業なしにこれを復旧することができます。とはいえ例え解読作業がないとしても実際にそれを復旧することは難しいので、本ソフトでは、対応する鍵コンテナの有無に関わらず、全ての証明書 BLOB を、現に稼動する Windows 上に復旧することができるようになっています。

尚、「C:\Users¥(ユーザー名)¥AppData¥Roaming」というロケーションは Windows Vista 以降のもので、Windows XP では「C:\Documents and Settings¥(ユーザー名)¥Application Data」となっています。以降、XP ではそのように読替えてください。Windows Vista 以降では XP で存在したこれらロケーションは実体としてはなくなりましたが、リンクで存在しているためファイルロケーションとしては依然有効です。

鍵コンテナ

Windows の鍵コンテナも、概念的にユーザーエリアかローカルマシンエリアに保存されますが、その実体 (KEYBLOB) は以下の場所に存在します。

ユーザーエリアの鍵コンテナ

C:\Users¥(ユーザー名)¥AppData¥Roaming¥Microsoft¥Crypto¥RSA\DSS¥S-1-5-?(ユーザーRPCSID)内の各ファイル
RPCSID とは各ユーザーに OS が割当てた一意な GUID で S-1-5 で始まる
生成される鍵によって RSA ないし DSS フォルダに分けられる 但しほとんどが RSA

ローカルマシンエリアの鍵コンテナ

C:\ProgramData¥Microsoft¥Crypto¥RSA\DSS¥MachineKeys 内の各ファイル
C:\ProgramData¥Microsoft¥Crypto¥RSA\DSS¥S-1-5-18 内の各ファイル
生成される鍵によって RSA ないし DSS フォルダに分けられる 但しほとんどが RSA

通常、ユーザーエリアの証明書にはユーザーエリアの鍵コンテナが対応しますが、それは通例なだけであって、原理的には証明書の場所と鍵コンテナの場所は別途独立なため、証明書はユーザーエリアで対応する鍵コンテナはローカルマシンエリアということ (その逆さえ) も有り得ることには注意が必要です。

鍵コンテナ内には署名鍵と鍵交換鍵の 2 種類の鍵が存在し得ます。そして、これら両方がある、両方が無い、片方だけ有るという状態が有り得ます。

そして、この各鍵コンテナ内の署名/鍵交換鍵それぞれの BLOB 内に、DPAPI で暗号化された、秘密鍵の BLOB とエクスポート可能フラグの BLOB が存在します。

鍵コンテナ内のこの他の情報は暗号化されていません。例えば公開鍵の情報は剥き出しです。

以降、DPAPI で暗号化された BLOB を DPAPIBLOB と称します。

そしてこの DPAPIBLOB を復号化することが本ソフトの主たる目的になります。

CREDHIST

DPAPI の復号化に時として必要となるファイルです。これはユーザーモード DPAPI でのみ使われます。

内容はそのユーザーの過去のログインパスワードと RPCSID の履歴です。各履歴エントリには、パスワードそのものが記録されているわけではなく、パスワードの SHA1 ハッシュと MD4 ハッシュが記録されています。

そのユーザーがパスワードを一度も変更したことがなければ CREDHIST ファイルの内容はほぼ空のエントリが一つあるだけの状態になります。現在のパスワードハッシュは CREDHIST には記録されません。

過去のパスワードハッシュエントリは特殊な暗号化が施されており復号化が必要ですが、本ソフトはもちろんそれを解読します。但しこの解読には最低限、現在のパスワードが必要です。

CREDHIST の場所は

C:\Users¥(ユーザー名)¥AppData¥Roaming¥Microsoft¥Protect 内のファイル「CREDHIST」となります。
ユーザーモード DPAPI の復号化に現在のユーザーパスワード (正確にはその SHA1 ハッシュか MD4 ハッシュ) は必須ですが、必ずしも過去のそれは必要なく、CREDHIST は例外的にしか使われません。
詳細は後段の「MASTERKEY」で説明します。

MASTERKEY

DPAPI の復号化時に絶対的に必要となるファイルです。

場所は

ユーザーモード DPAPI の MASTERKEY ファイル

C:\Users\%(ユーザー名)\AppData\Roaming\Microsoft\Protect\S-1-5-(各ユーザーRPCSID)内の各ファイル
ローカルマシンモード DPAPI の MASTERKEY ファイル

C:\Windows\System32\Microsoft\Protect\S-1-5-18 内の各ファイル

C:\Windows\System32\Microsoft\Protect\S-1-5-18\User 内の各ファイル
となります。

MASTERKEY(ファイル)は複数あります。DPAPI で暗号化された DPAPIBLOB の中にはどの MASTERKEY を使って暗号化されたのかの情報が、それをもとに使うべき MASTERKEY が決定されます。

MASTERKEY ファイルの中には DPAPI の暗号化/復号化に使う鍵(これが正に MASTERKEY)および DPAPI 暗号方法に関する情報が入っていますが、この鍵は CREDHIST 内での暗号化と似たような(似ているだけで同じではありません)方法で暗号化されています。この暗号解読が一番厄介で、この MASTERKEY さえ取り出せば後の DPAPI 解読は簡単です。

MASTERKEY を解読するには、

ユーザーモードの DPAPI では

ローカルマシンユーザーでは、そのユーザーの RPCSID とログインパスワードの SHA1 ハッシュ

ドメインユーザーでは、そのユーザーの RPCSID とログインパスワードの MD4 ハッシュ

マイクロソフトアカウントでは、

そのユーザーの RPCSID とログインパスワードの MD4 ハッシュと

レジストリ HKEY_LOCAL_MACHINE\SAM 内の情報から導かれる KEY

ユーザーモードの DPAPI で、もし現在のパスワードで MASTERKEY の解読に失敗した場合は
CREDHIST から過去のパスハッシュを取得し順次それらで解読を試みます。

ローカルマシンモード DPAPI では

レジストリ HKEY_LOCAL_MACHINE\SYSTEM 及び SECURITY 内の情報から導かれる DPAPI_SYSTEM_KEY

が必要になります。

尚、上記レジストリとそれに対応する実体ファイルの対応は以下です。

HKEY_LOCAL_MACHINE\SAM C:\Windows\System32\config\SAM

HKEY_LOCAL_MACHINE\SYSTEM C:\Windows\System32\config\SYSTEM

HKEY_LOCAL_MACHINE\SECURITY C:\Windows\System32\config\SECURITY

本ソフトはこれらレジストリ情報を取得するに、実体ファイル(のテンポラリコピー)を現稼働中の Windows システムのレジストリ HKEY_USERS 以下に暫定接続させ、アクセス権を調整しながら読み取っています。

現稼働中の C:をターゲットにした場合、C:\Windows\System32\config\SAM 等を読みに行くことになりませんが、OS が稼働中はこれら SAM や SYSTEM、SECURITY のファイルをダイレクトに読むことはできないため、Windows の VolumeShadowCopyService (VSS)を使ってコピーしてそれを行っています。

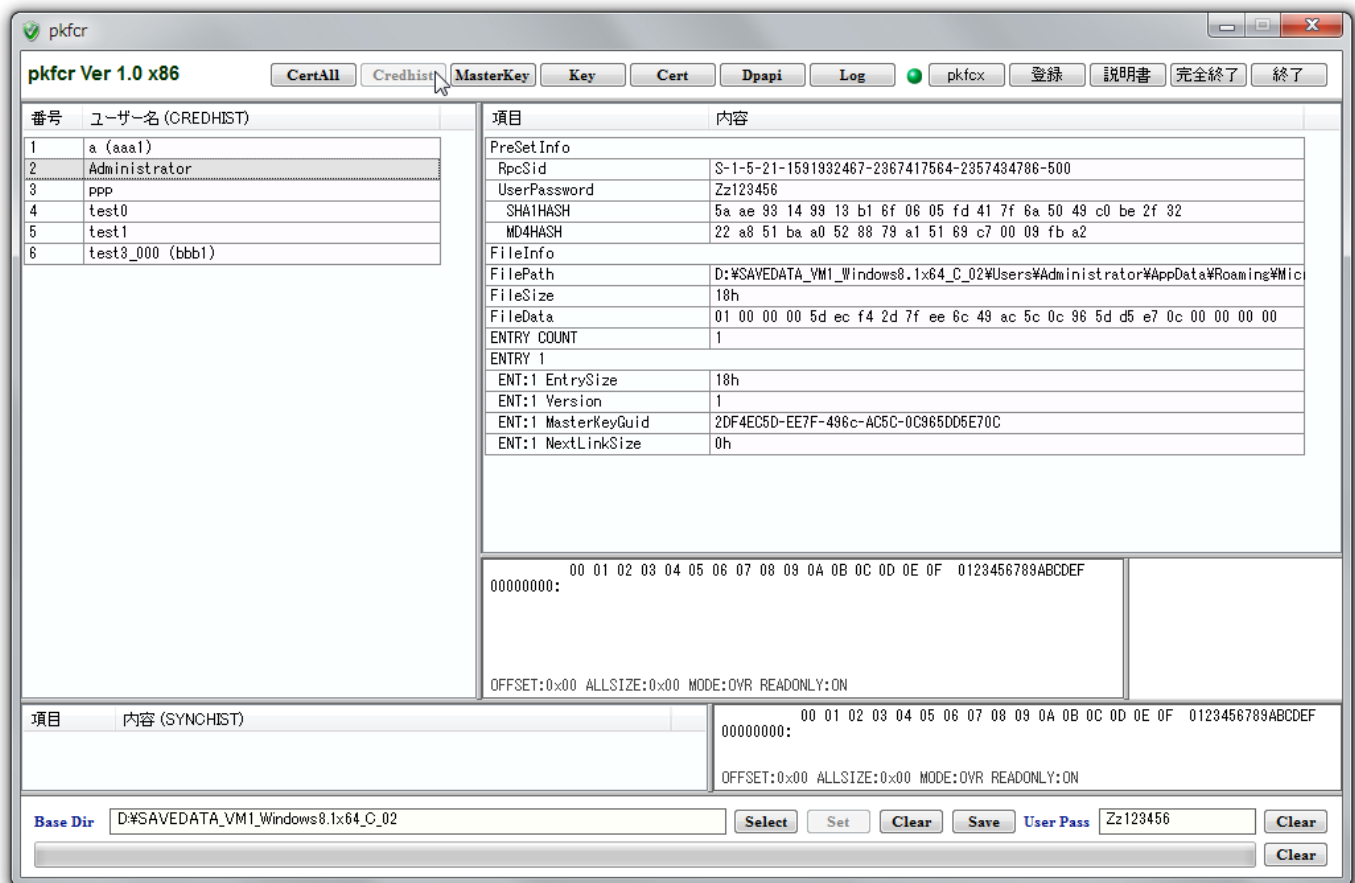
各操作画面の詳細

先の操作方法説明は「pkfcr」の第1ページ「CertAll」での簡単操作についてでした。「pkfcr」にはこの他に、突っ込んだ個別的处理ができる各画面が用意されていますので、以下ではこれら各画面の操作方法を説明します。各画面には、以下があります。

「CertAll」	証明書復旧を視覚的に簡単自動操作で行う画面
「Credhist」	「CREDHIST」を取り扱う画面
「MasterKey」	「MASTERKEY」を取り扱い、個別に復号化を行う画面
「Key」	「鍵コンテナ(BLOB)」を取り扱い、個別に復号化を行う画面
「Cert」	「証明書(BLOB)」を取り扱い、個別に復旧構成設置を行う画面
「Dpapi」	指定のディレクトリ内全ファイルから「DPAPI」BLOB を探し出し、個別に解読する画面
「Log」	全ての処理について、ログを出力する画面

CREDHIST 画面

画面上部「Credhist」ボタンを押すと現れるのは、先に説明した「CREDHIST」を扱う画面です。「基本ディレクトリ」で選択されたターゲット内に存在する全てのユーザーの CREDHIST が表示されます。



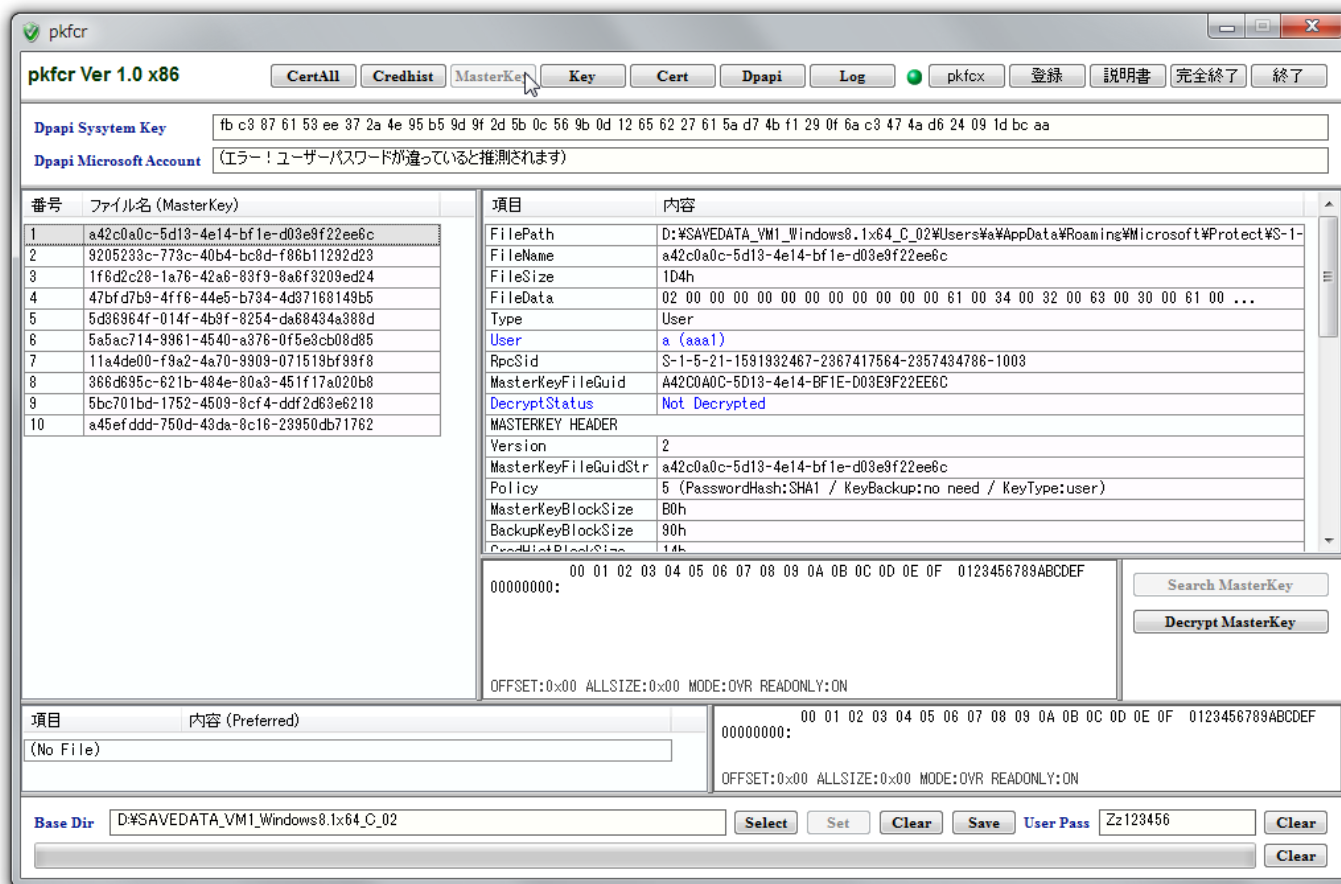
画面下部右方の UserPass に設定されたユーザーパスワードに従い、各ユーザーの「CREDHIST」ファイルを解読して表示します。上図の例ではユーザー「Administrator」の「CREDHIST」ファイルの内容が表示されています。この例では「ENTRY」が1つしかないので特に暗号化された部分はありません。「CREDHIST」ファイルでは、ユーザーがパスワードを変更するたびに「ENTRY」が1つずつ増えていきます。そして2つ目以降の「ENTRY」には過去のRPCSIDと暗号化された過去のパスワードのハッシュが保存されます。それを解読するにはそのユーザーの現在のRPCSIDとログインパスワードが必要になります。

上図の右方で「PreSetInfo」と表示されている数行は、正確には「CREDHIST」ファイルの内容ではありません。これはこの「CREDHIST」ファイルの解読に使った、現在のRPCSIDとパスワードを表示しているにすぎません。「CREDHIST」ファイルの内容は「FileInfo」以下の行になってきます。

「DPAPI」を解読するにほとんど「CREDHIST」ファイルが使われることはありません。よってこの画面はそれほど重要ではありません。

MASTERKEY 画面

画面上部「MasterKey」ボタンを押すと現れるのは、先に説明した「MASTERKEY」を扱う画面です。「基本ディレクトリ」で選択されたターゲット内に存在する全てのユーザーの全ての MASTERKEY が表示されます。



「Dpapi System Key」とは、LocalMachine の MASTERKEY を解読するために必要なレジストリの SYSTEM と SECURITY から導かれる Key です。

「Dpapi Microsoft Account (Key)」とは Windows8 以降のマイクロソフトアカウントユーザーの MASTERKEY を解読するに必要なレジストリの SAM から導かれる Key です。上図で左方リストで選択されている MASTERKEY がマイクロソフトアカウントユーザーのものである場合、画面右方下部の UserPass にそのユーザーの正しいパスワードが設定されていないと、上図のように(エラー！・・・)と表示されます。ここで(ユーザーaaa1 の)正しいパスワードを設定すれば、この Key が表示されるようになります。

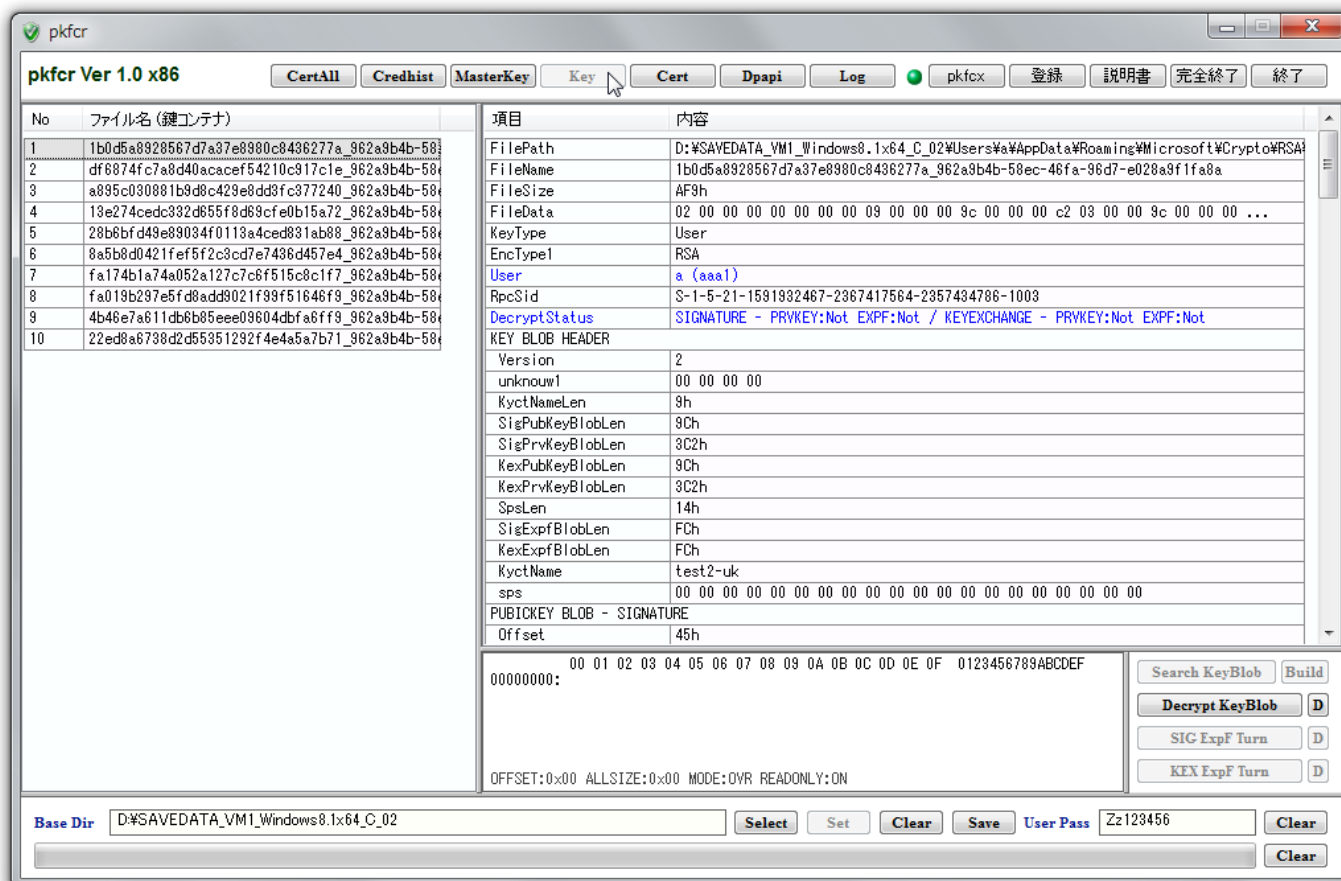
画面右方の「Decrypt MasterKey」ボタンは、現在左方リストで選択されている MASTERKEY の解読を行います。

「Search MasterKey」ボタンは、次で説明する「Key(鍵コンテナ)」画面で選択されている鍵コンテナを解読するために必要な対応 MASTERKEY を本ページで探索するものです。「Key(鍵コンテナ)」ページで何か鍵コンテナが選択されていないと有効化しません。

画面下方の「Preferred」とは MASTERKEY が存在するディレクトリに存在する「Preferred」ファイルの内容を表示するもので、MASTERKEY は(各ユーザー毎に)複数存在し得ますが、原則現在の DPAPI で使用される MASTERKEY は最新のひとつであるところ「Preferred」はその現在有効な MASTERKEY を示すファイルとなります。あまり重要なものではありません。

KEY 画面

画面上部「Key」ボタンを押すと現れるのは、先に説明した「鍵コンテナ(BLOB)」を扱う画面です。「基本ディレクトリ」で選択されたターゲット内に存在する全てのユーザーの全ての鍵コンテナが表示されます。



画面右方の「Decrypt KeyBlob」ボタンは、選択している鍵コンテナを解読します。

「Search KeyBlob」ボタンは、次で説明する「Cert(証明書)」画面で選択されている証明書に対応する鍵コンテナを本ページで探索するものです。「Cert(証明書)」ページで何か証明書が選択されていないと有効化しません。

「Build」ボタンは、選択されかつ解読済みの鍵コンテナを現稼動システムに登録するものです。

「SIG Exp Turn」ボタンは、選択されかつ解読済みの鍵コンテナの署名鍵の秘密鍵のエクスポート可能フラグを反転するものです。「KEX Exp Turn」ボタンは、選択されかつ解読済みの鍵コンテナの鍵交換鍵の秘密鍵のエクスポート可能フラグを反転するものです。

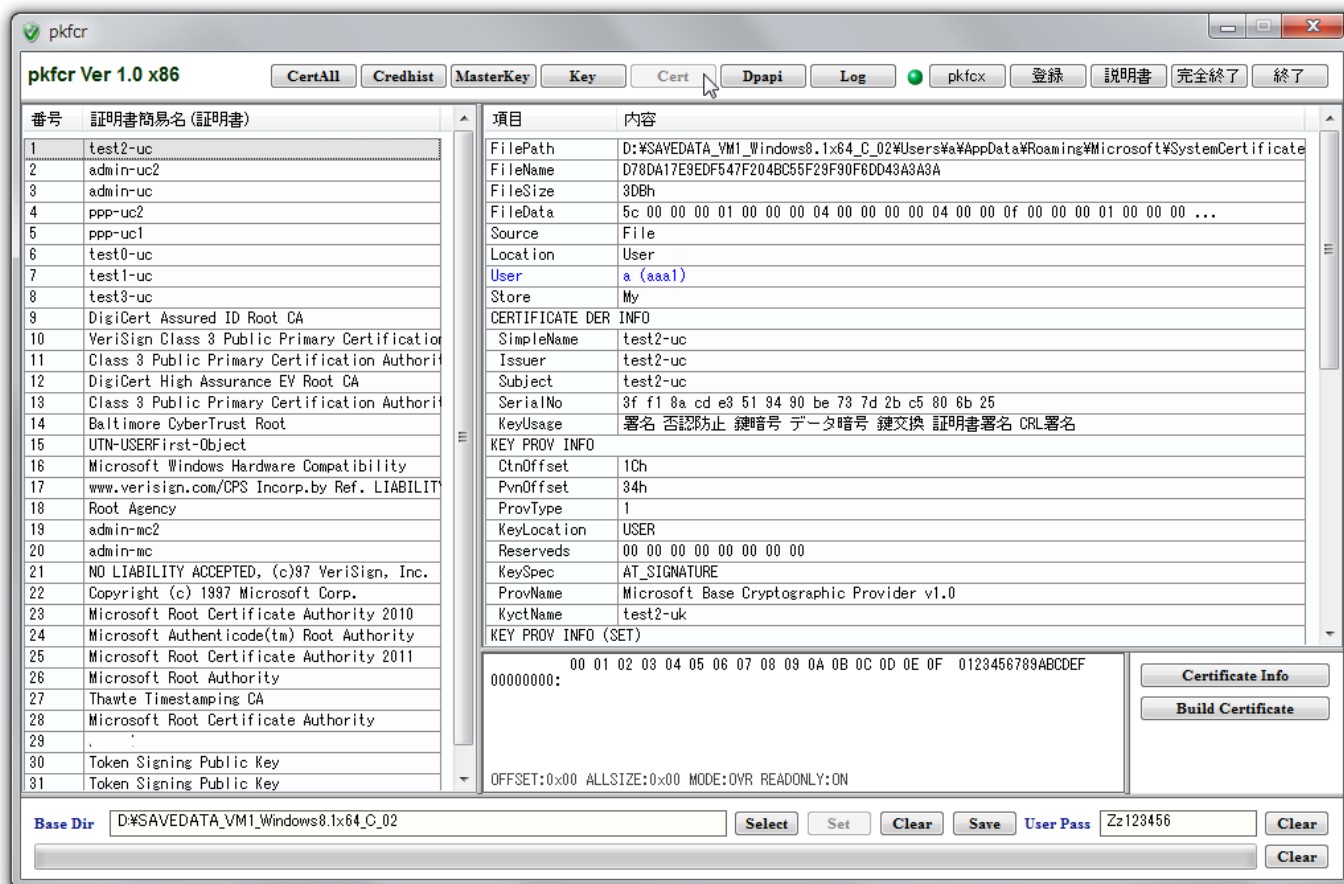
「Decrypt KeyBlob」ボタン右の「D」ボタンは、現稼動中のシステムの DPAPI を使って現在選択されている鍵コンテナを解読するものです。「基本ディレクトリ」で「C:ドライブ」を選択していない限り、現稼動中のシステムの DPAPI では通常、鍵コンテナを解読はできないため、この機能はテスト的なものです。

「SIG Exp Turn」ボタン右の「D」ボタンは、現稼動中のシステムの DPAPI を使って現在選択されている鍵コンテナの署名鍵の秘密鍵のエクスポート可能フラグを反転するものです。これも上に同じでテスト的なものです。

「KEX Exp Turn」ボタン右の「D」ボタンも、現稼動中のシステムの DPAPI を使って現在選択されている鍵コンテナの鍵交換鍵の秘密鍵のエクスポート可能フラグを反転するものです。これも上に同じでテスト的なものです。

CERT 画面

画面上部「Cert」ボタンを押すと現れるのは、先に説明した「証明書(BLOB)」を扱う画面です。「基本ディレクトリ」で選択されたターゲット内に存在する全てのユーザーの全ての証明書が表示されます。

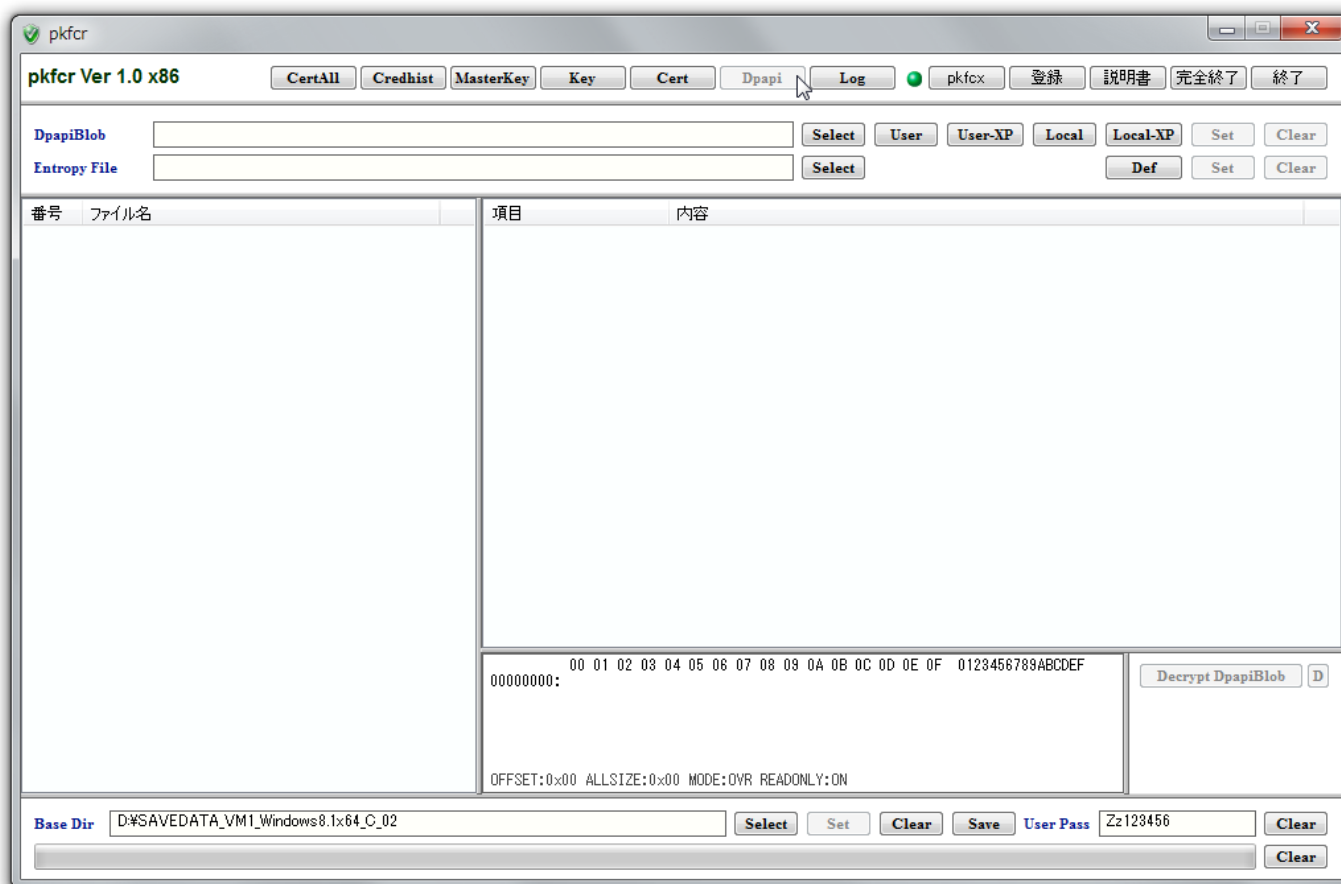


「Certificate Info」ボタンは、現在左方リストで選択されている証明書の現稼動中の Windows 証明書としての情報を表示します。ここで選択されている証明書は現稼動システムに正規に登録されているわけではないので、一部の内容は正確ではありませんが、証明書の詳細を掴むことができます。

「BuildCertificate」ボタンは、選択されている証明書を現稼動システムに登録します。

DPAPI 画面

画面上部「Dpapi」ボタンを押すと現れるのは、「DPAPI (BLOB)」を個別に扱う画面です。



基本的に DPAPI で暗号化されたと思われるファイルが存在するディレクトリを「Select」で選択します。

「User」ボタンは、現稼動システム上の現在のユーザーの RSA 系の鍵コンテナファイルが存在するディレクトリを自動で選択します。「User-XP」ボタンは、WindowsXP システムで上記ユーザー鍵コンテナファイルが存在するディレクトリを自動選択します。

「Local」ボタンは、現稼動システム上のローカルマシンエリアの RSA 系の鍵コンテナファイルが存在するディレクトリを自動で選択します。「Local-XP」ボタンは、WindowsXP システムで上記ローカルマシン鍵コンテナファイルが存在するディレクトリを自動選択します。

「Set」ボタンは上記で選択した場所にターゲットファイルが存在する場合に有効化し、それを押すと選択したディレクトリ内の全ファイル中の全 DPAPIBLOB を探し出し表示します。

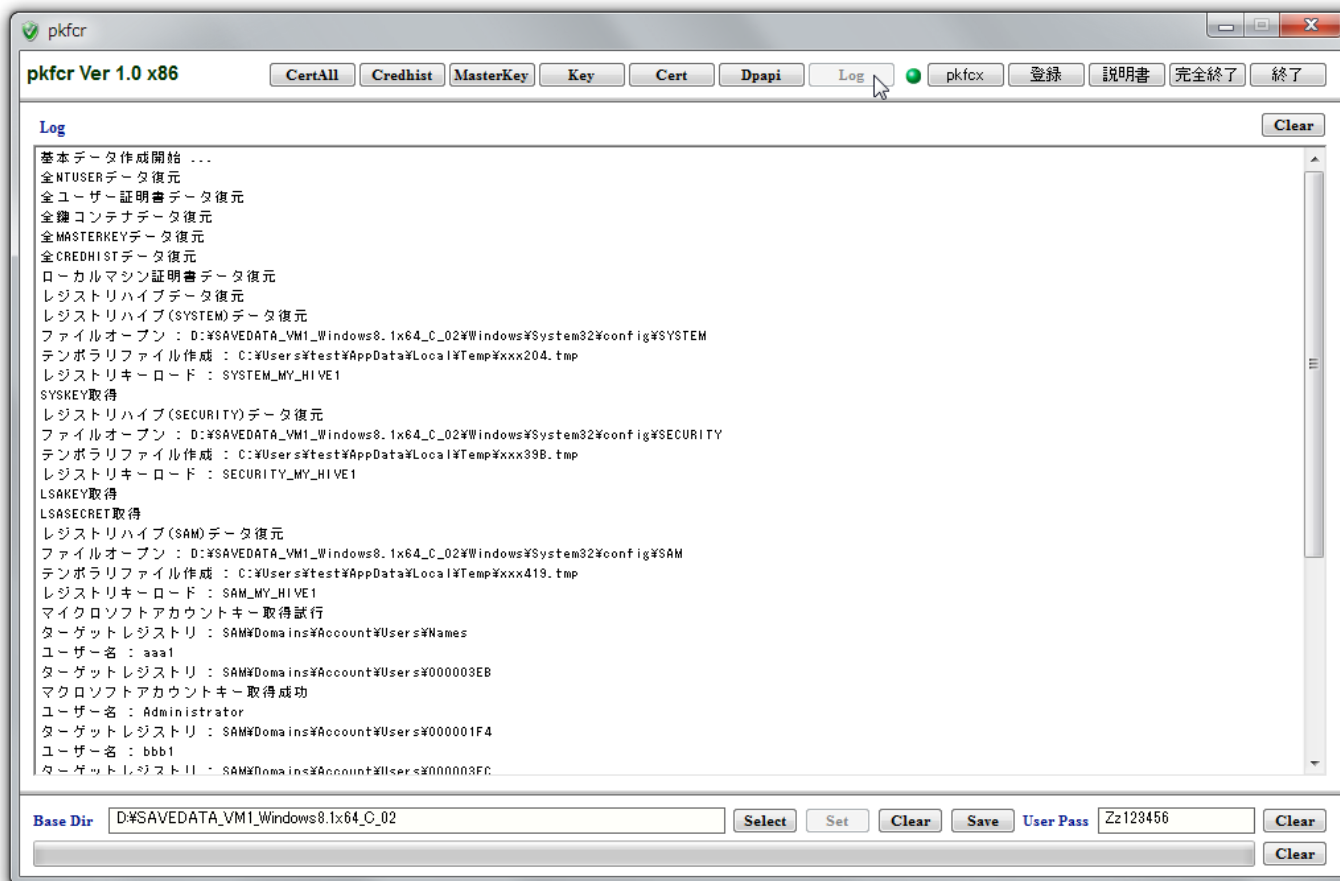
「Entropy File」は DPAPI を解読するに追加に必要なバイナリデータを記録したファイルを選択します。DPAPI では暗号化を施すときに追加データとして「Entropy」を指定することができます。そのような Entropy データを使って暗号化された DPAPIBLOB を復号化するには、暗号化時に使ったのと同じ Entropy データが必要になります。もしそれが必要ならば自前でそれを作りここで提供する必要があります。

ちなみに鍵コンテナの秘密鍵エクスポートフラグの DPAPIBLOB の解読には一定の Entropy データが必要ですが、これについては本ソフトが自動で判断しそれを内部的に提供しますので、これについてはEntropyFileは必要ありません。右方の「Select」ボタンでファイルを選択します。「Def」ボタンは「基本ディレクト」直下の「EntoropyData」という名前のファイルを選択します。「Set」ボタンで Entoropy データをセットします。「Clear」ボタンはこれらの解除となります。

中段右方の「Decrypt DpapiBlob」ボタンは、復号化を実行します。その右の「D」ボタンは現稼動中のシステムの DPAPI での解読を試みますが、これがテスト的なものである点は、「Key(鍵コンテナ)」画面の「D」ボタンと同様です。

LOG 画面

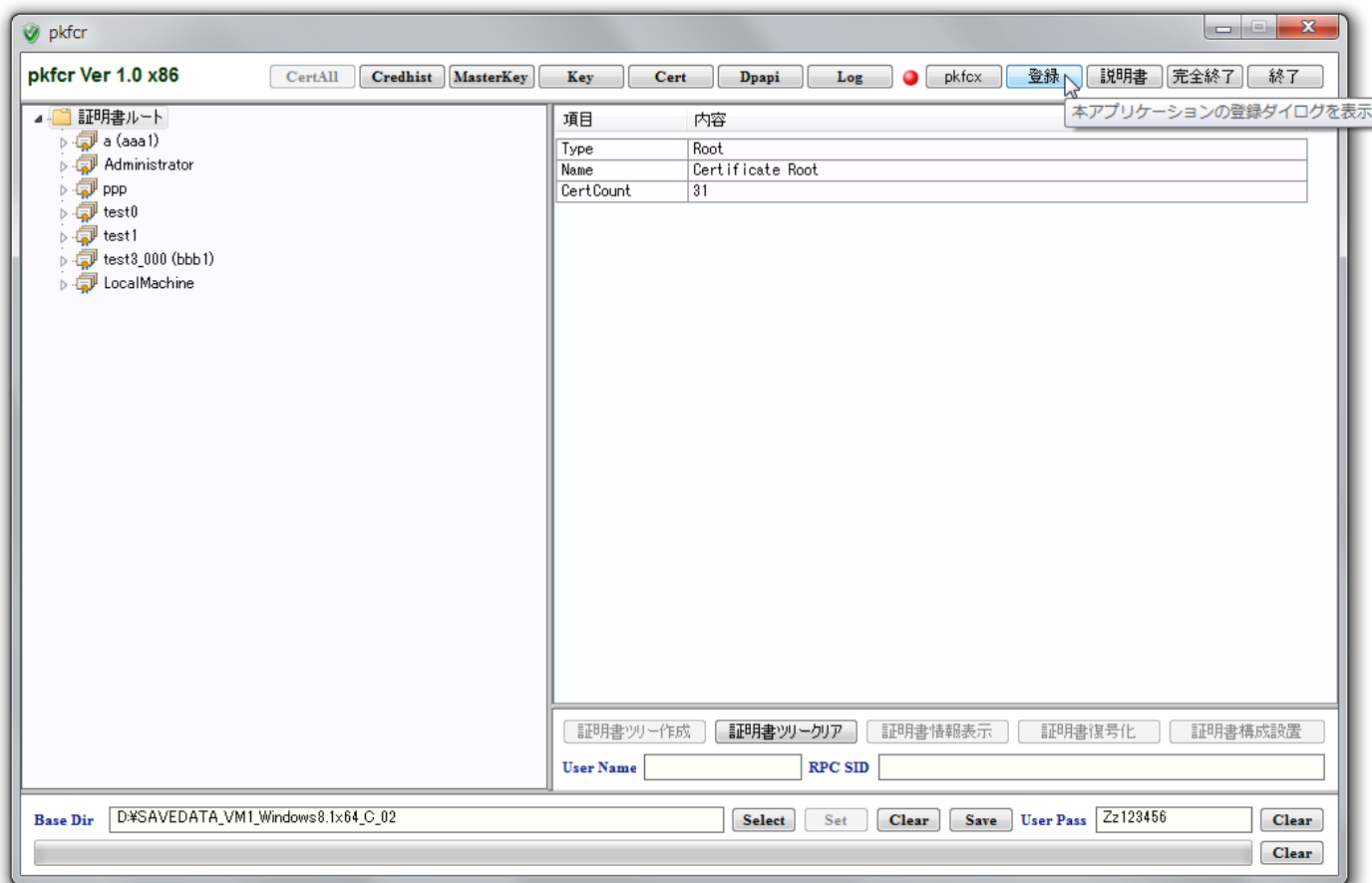
画面上部「Log」ボタンを押すと現れるのは、ログを表示する画面です。



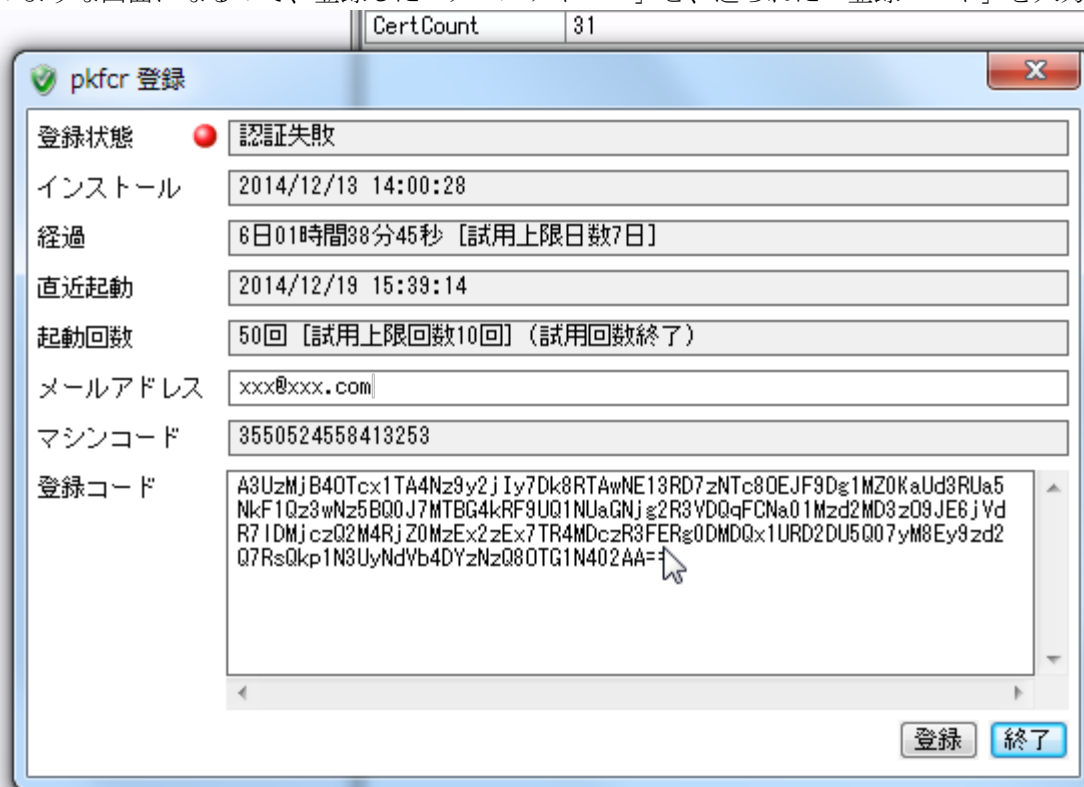
「pkfcr」での種々のアクションにつき一定の情報を表示します。通常これを見る必要はありません。画面上方右方の「Clear」ボタンでログはクリアされます。

(購入) 登録方法

登録方法を説明します。画面上部の「登録」ボタンを押します。



このような画面になるので、登録した「メールアドレス」と、送られた「登録コード」を入力します。



「マシンコード」はここでは関係ないので無視してください。

「インストール」日時、「直近起動」日時、「起動回数」は継続的に記録されていきます。

「登録」ボタンを押します。正しい「登録コード」が入力されていれば「認証完了」となります。

The screenshot shows the 'pkfcr Ver 1.0 x86' application window. At the top, there are several tabs: 'CertAll', 'Credhist', 'MasterKey', 'Key', 'Cert', 'Dpapi', 'Log', 'pkfcx', '登録' (highlighted in blue), '説明書', '完全終了', and '終了'. Below the tabs is a table with two columns: '項目' (Item) and '内容' (Content). A modal dialog titled 'pkfcr 登録' is open in the center. It displays the following information:

- 登録状態: 認証完了 (with a green checkmark icon)
- インストール: 2014/12/13 14:00:28
- 経過: 6日05時間15分21秒
- 直近起動: 2014/12/19 19:15:50
- 起動回数: 51回
- メールアドレス: xxx@xxx.com
- マシンコード: 3550524558413253
- 登録コード: A3UzMjB4OTcx1TA4Nz9y2jiy7Dk8RTAwNE13RD7zNTc8OEJF9Dg1M20KaUd3RUa5NkF1Qz3wNz5B00J7MTBG4kRF9UQ1NUaGNJz2R3YDQqFCNa01Mzd2MD3z09JE6jVdR71DMjczQ2M4RjZ0MzEx2zEx7TR4MDczR3FERg0DMDQx1URD2DU5Q07yM8Ey8zd2Q7RsQkp1N3UyNdYb4DYzNzQ80TG1N402AA==

At the bottom of the dialog, there are '登録' and '終了' buttons. A tooltip over the '登録' button says '現在入力表示されている内容で登録します'. Below the dialog, there are input fields for 'User Name' and 'RPC SID', and a '現在入力表示されている内容で登録します' button. At the very bottom, there are fields for 'Base Dir' (D:\SAVEDATA_VM1_Windows8.1x64_C_02), 'Select', 'Set', 'Clear', 'Save', 'User Pass' (Zz123456), and 'Clear' buttons.

登録後は画面上方のマークが上図のとおり緑色になります。
このマークは試用中は黄色、試用期間回数切れの場合は赤色、登録時は緑色になります。

その他

① ローカルマシンエリアの証明書を扱うときの注意

ローカルマシンエリアに保存される証明書は、レジストリの HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\MY\Certificates 等に入りますが、新しくローカルマシンエリアに証明書を入れた直後は(例えば OS 再起動するまでは)、これに対応する実体の C:\Windows\System32\config\SOFTWARE ファイルに(時間的に)なかなか反映されません。レジストリへの変更は、直ちにはシステムの該当ファイルに反映されないのです(API の RegFlushKey を実行しても)。反映されない内にこの「SOFTWARE」ファイルをバックアップすると、当然に反映前の状態しか取得できません。ある環境で、ローカルマシンエリアに保存される証明書を扱った(新規作成等)場合で、レジストリファイル「SOFTWARE」をバックアップしようとするとき(pkfcr の「全データセーブ」を「C:ドライブ」に対し実行するとき)は、一度「OS 再起動」する必要があります。

② 「pkfcr」での VSS (VolumeShadowCopyService) について

VSS では各ドライブの初期化(スナップショット取得)に少々時間が掛かります。本アプリケーション起動中は、一度 VSS 初期化処理したドライブは、二度目からは「保持」しているスナップショットを使うため時間が掛かりませんが、WindowsXP のみこの「保持」ができないため、毎回初期化を行います。よって XP で VSS 処理が必要となる場合、異常に処理に時間が掛かります。

③ VMWare の仮想ディスクとネットワークドライブ割当て

もし VMWare の仮想ディスクを pkfcr の復旧対象としようとする場合、VMWare のツールを使いその仮想ディスクをドライブマップするのが通例と思いますが、このとき若干の注意が必要です。ネットワークドライブの割当て時のドライブレター割当ては、ユーザー個別なだけでなく、同じユーザーでも昇格(elevated) (いわゆる「管理者として実行」)した状態と、そうでない状態(通常の実行)では別となります。VMWare の仮想ディスクをドライブ Z: にマップしたとき、通常それは非昇格のユーザーで行われるため、Windows の Explorer であれば普通にそれが見れるところ(このとき Explorer を「管理者として実行」してもその Explorer は非昇格で実行されるため、やはり見れます)、昇格する本ソフトからはそれ(Z: ドライブ)が見えない状態になります。これを避けるためには VMWare 等のドライブマップするプロセスを「管理者として実行」する必要があります。尚この時、VMWare では自動で開く Explorer から Z: ドライブがエラーで見えなくなります。これは Z: が昇格ユーザーのコンテキストにマップされているところ、Explorer プロセスが非昇格ユーザープロセスで実行されているため、それが見えない状態になっているわけです。